WHITE PAPER

now from symantec VERITAS

VERITAS NetBackup™ 6.0 Technical Overview

VERITAS NETBACKUP™ 6.0 TECHNICAL OVERVIEW
UNABRIDGED VERSION

(Updated as of NetBackup 6.0 Release, June 2005)

TABLE OF CONTENTS

VERITAS NETBACKUP™ PRODUCT OVERVIEW

VERITAS NetBackup Enterprise Server delivers high performance data protection that scales to protect the largest UNIX, Windows, Linux and NetWare environments. Offering complete protection from desktop to data center to vault, NetBackup software offers a single management tool to consolidate all backup and recovery operations, while providing cutting-edge management, alerting, reporting, and troubleshooting technologies. NetBackup helps organizations take advantage of both tape and disk storage with its advances in disk and snapshot-based protection, off-site media management, and automated disaster recovery. For the ultimate in data protection, NetBackup offers data encryption that transmits and stores data using the latest encryption technologies on the market today. To reduce the impact on business critical systems, NetBackup software provides online database and application aware backup and recovery solutions for all leading databases and applications.

The NetBackup Desktop and Laptop Option is designed to provide a scalable and practical solution for centrally managing the backup of desktops and laptops within a corporate environment. The NetBackup Desktop and Laptop Option will be discussed in a separate white paper, and additional information can be found on the VERITAS Web site at www.veritas.com.

KEY AREAS OF FOCUS FOR NETBACKUP 6.0

VERITAS NetBackup 6.0 contains many new features and enhancements designed to increase the scalability and functionality of NetBackup to address the requirements of large enterprise customers.

Key areas of focus are as follows:

- Further enhance NetBackup software's disk backup and recovery capabilities.
- Collaborate with Network Appliance to differentiate NetBackup from the competition by providing support to back up data directly to NetApp’s NearStore appliance.
- Improve NetBackup management and reporting.

VERITAS continues to improve NetBackup in the areas of scalability, improved disk backup capabilities, and product integration. The following list identifies many of the new NetBackup 6.0 features and enhancements that will be available to NetBackup users:

- NetBackup Advanced Client Enhancements
- NetBackup Bare Metal Restore (BMR)
  - → Integration with NetBackup
  - → Linux client support
  - → Support for VERITAS Foundation Suite
- NetBackup Database Agent Enhancements
  - → SAP backup integration with Oracle RMAN
  - → Lotus Notes agent
  - → Microsoft SQL Server 2005 support
  - → SharePoint 2003
- NetBackup Disk Based Data Protection Capabilities
  - → Network Appliance NearStore Disk Storage Unit
  - → Network Appliance SnapVault Disk Storage Unit
  - → Disk backup performance
  - → Leverage Disk Storage Unit (DSU) groups
- NetBackup Media Manager
  - → Enterprise Media Manager (EMM)
  - → Multi-path Shared Storage Option (SSO)
  - → Enhanced Device Discovery for ACS and TLM Robotics
  - → Media Manager scalability

- NetBackup core enhancements
  → Intelligent Resource Manager (IRM)
  → Port Reduction
  → NetBackup catalog enhancements
- NAS and NDMP
  → NetApp SnapVault integration
  → Simplified snapshot setup
- NetBackup Operations Manager provides management and reporting enhancements

Many of the key NetBackup 6.0 key features listed above will be described in more detail in this document. Other supporting white papers that discuss these features in detail will be created by VERITAS and will be made available.

OTHER KEY FEATURES OF NETBACKUP

VERITAS NetBackup software's key features include disaster recovery support and intuitive Java and Windows administrative interfaces. Other key features include synthetic backup, disk staging, the Advanced Client and Checkpoint/Restart for backups and recoveries. In addition to protecting data in mixed UNIX, Linux, Microsoft Windows and Novell NetWare environments, VERITAS NetBackup software delivers advanced, "application aware" solutions for all leading applications including Oracle, IBM DB2, SAP, Microsoft SQL Server, Microsoft Exchange Server, Microsoft SharePoint Portal Server, Lotus Notes & Domino Server, Informix and Sybase. VERITAS NetBackup software provides high performance backup, archiving, and recovery services for UNIX, Linux, Windows, and PC client systems in client/server networks. It can be economically scaled to serve any size operation ranging from a standalone system to an entire enterprise.

Administrators can set up periodic or calendar-based schedules for automatic, unattended backup operations of clients across the network. These backup operations may be full or incremental. A full backup processes all files, while an incremental backup only processes those files changed since the last full or incremental backup. By carefully scheduling automatic backups, an administrator can achieve systematic and complete backups over a period of time, and optimize network traffic during off-peak hours.

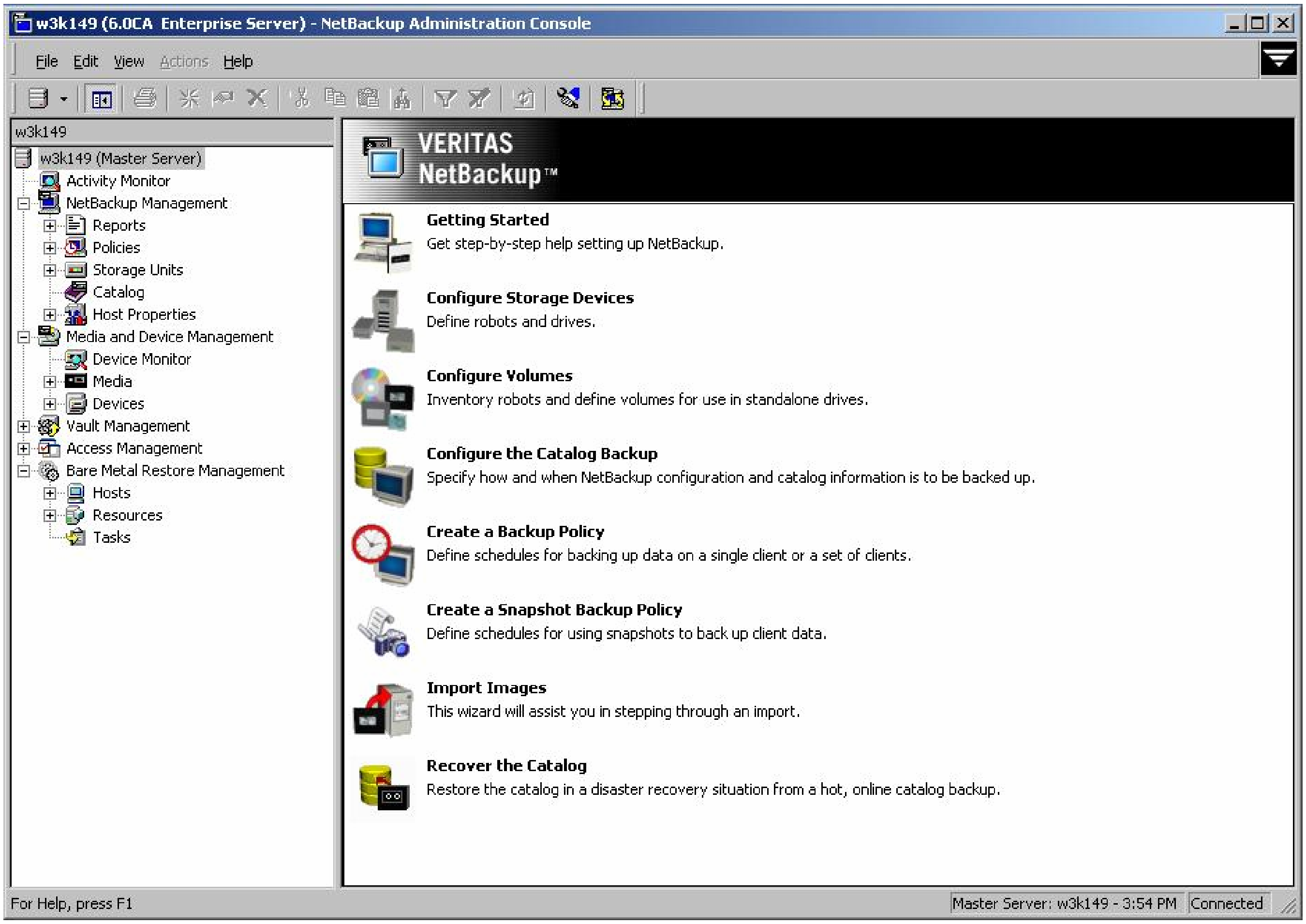
Synthetic backups may be required for NetBackup users that require quick restores and backups that do not put a heavy workload on their network. Synthetic backups are automatically created from one full backup or a synthetic full backup and any number of incremental backups. Synthetic backups allow for quick client restore from a single backup image. Synthetic backups consume less network bandwidth and decrease the impact on the application host.

In addition to scheduled backups, administrators can perform manual backups of client data using the same criteria as specified for automatic backups. Manual backup operations are useful in special circumstances, such as backing up a client that missed a previously scheduled backup or preserving a system configuration prior to installing new software.

NetBackup client users are able to initiate backup, archive, and restore operations for data on their client systems without operator or administrator intervention. User-directed backups allow the user to protect their files immediately on demand. If files are damaged or accidentally deleted, users can quickly and easily recover any backed up or archived files by restoring them back to their primary disk space.

NETBACKUP ADMINISTRATION CONSOLE

The NetBackup Administration Console, as shown in Figure 1 below, provides an easy, intuitive entry point into NetBackup software's administration categories. Primary administration is separated into five management areas: NetBackup Management, Media and Device Management, Vault Management, Access Management and Bare Metal Restore Management. Under NetBackup Management, the administrator may run reports, create backup policies and storage units, manage the catalog, or configure host properties for master servers, media servers or clients. Within Media and Device Management, the NetBackup user manages tape media and devices, from the creation of tape media groups and pools to the monitoring of tape devices. Vault Management extends media management to the automation and control of all facets of offsite tape vaulting. Access Management provides easy to use security for NetBackup. Bare Metal Restore Management allows the user to centrally manage machine recovery. In addition, the NetBackup Administration Console offers a variety of configuration wizards to simplify many routine tasks.



Getting Started
Get step-by-step help setting up NetBackup.

Configure Storage Devices
Define robots and drives.

Configure Volumes
Inventory robots and define volumes for use in standalone drives.

Configure the Catalog Backup
Specify how and when NetBackup configuration and catalog information is to be backed up.

Create a Backup Policy
Define schedules for backing up data on a single client or a set of clients.

Create a Snapshot Backup Policy
Define schedules for using snapshots to back up client data.

Import Images
This wizard will assist you in stepping through an import.

Recover the Catalog
Restore the catalog in a disaster recovery situation from a hot, online catalog backup.

For Help, press F1

Master Server: w3k149 - 3:54 PM

Connected

Figure 1: NetBackup Administration Console

NETBACKUP SERVERS AND CLIENTS

VERITAS NetBackup software includes both client and server software. Server software resides only on the platforms that manage the physical devices used for secondary storage. Client software resides on the individual client systems containing the data to be backed up. For example, a server can also be a client in a NetBackup environment. In this architecture, client software is responsible for generating the data stream to be backed up and server software directs this data stream to a secondary storage device.

NETBACKUP CENTRALIZED MANAGEMENT

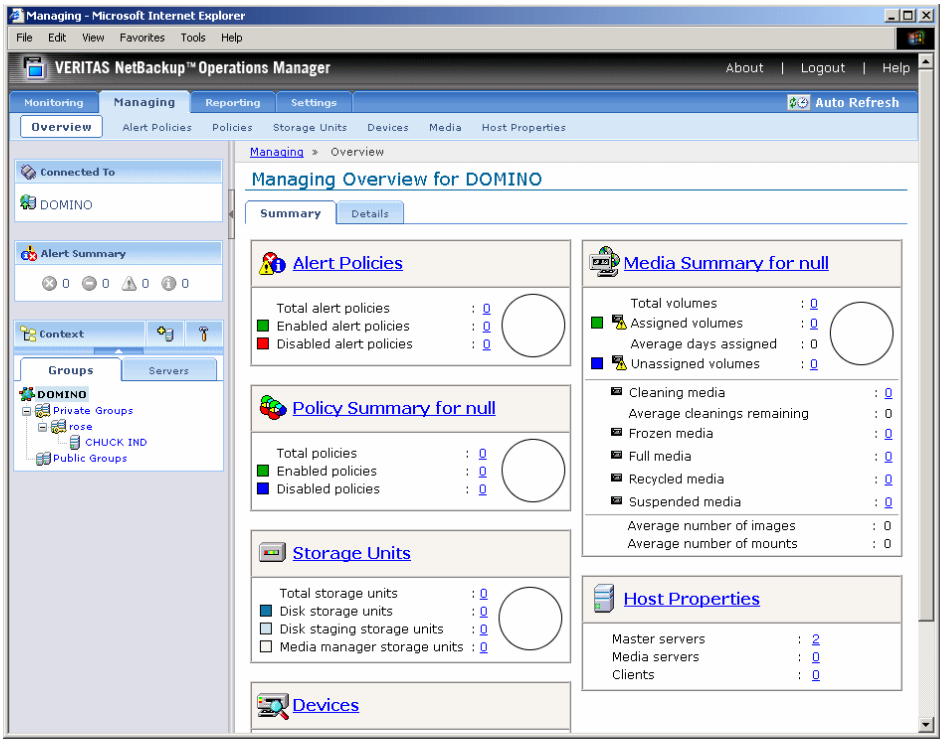
VERITAS NetBackup™ software accommodates multiple servers working together under the administrative control of one of the servers. In this relationship, the NetBackup administrative control server is designated to be the “master” server, with the other servers designated as “media” servers, operating under control of the master server. Please note that a master server can also function as a media server. All NetBackup administrative functions are performed centrally from the master server, and the master server controls all backup scheduling for each media server. Each of the media servers performs the actual backup operations under direction from the master, and backup data stays local to the media servers and their respective storage devices. A master server and its associated media servers are referred to collectively as a NetBackup storage domain, and large networks may have more than one domain. Client systems back up data to NetBackup servers.

VERITAS NetBackup Operations Manager

In environments where multiple local or remote NetBackup domains are implemented, VERITAS NetBackup Operations Manager (NOM) may be used to greatly simplify monitoring and reporting tasks. Operations Manager is a NetBackup core feature that provides centralized management, monitoring and reporting for multiple NetBackup domains across a corporate campus or around the world.

Operations Manager uses a web-based user interface to provide active management of the NetBackup environment. Information available includes but is not limited to basic drive control, job control, policy management and log management across multiple NetBackup master servers.

Operations Manager delivers enhanced management and monitoring functionality by extracting pertinent information from each unique NetBackup master server. Once Operations Manager has collected information for an entire NetBackup domain, users may look at their environment as a whole or may drill-down into specific NetBackup master servers. The Operations Manager console then presents not only NetBackup configuration and deployment details, but also a variety of real-time statistics, including details on failed jobs within the last 24 hours or completed jobs within the last 24 hours.



Managing Overview for DOMINO

Alert Policies

Total alert policies : 0
Enabled alert policies : 0
Disabled alert policies : 0

Policy Summary for null

Total policies : 0
Enabled policies : 0
Disabled policies : 0

Storage Units

Total storage units : 0
Disk storage units : 0
Disk staging storage units : 0
Media manager storage units : 0

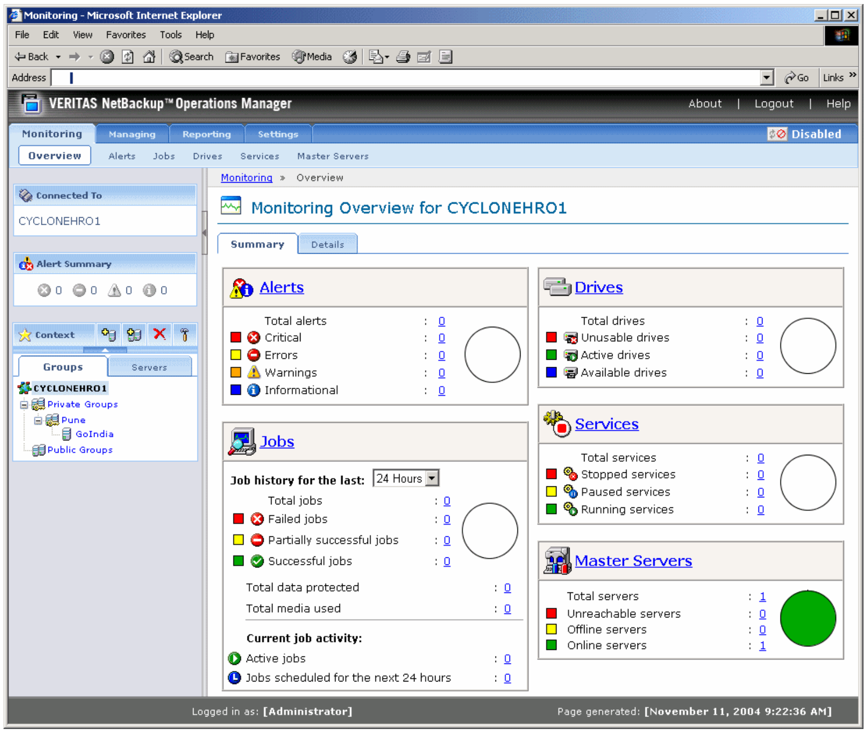
Media Summary for null

Total volumes : 0
Assigned volumes : 0
Average days assigned : 0
Unassigned volumes : 0
Cleaning media : 0
Average cleanings remaining : 0
Frozen media : 0
Full media : 0
Recycled media : 0
Suspended media : 0
Average number of images : 0
Average number of mounts : 0

Host Properties

Master servers : 2
Media servers : 0
Clients : 0

Figure 2: The NetBackup Operation Manager’s centralized web based interface provides a single management view of all NetBackup servers in the user’s worldwide enterprise.


Monitoring - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
VERITAS NetBackup™ Operations Manager
About | Logout | Help
Monitoring Managing Reporting Settings
Disabled
Overview Alerts Jobs Drives Services Master Servers
Connected To
Alert Summary
Context
Groups Servers
CYCLONEHRO1
Private Groups
Pune
GoIndia
Public Groups
Monitoring » Overview
Summary Details

CYCLONEHRO1

0 0 0 0

Monitoring Overview for CYCLONEHRO1

Alerts

Total alerts : 0
🟥 Critical : 0
🟨 Errors : 0
🟧 Warnings : 0
🟦 Informational : 0

Jobs

Job history for the last: 24 Hours

Total jobs : 0
🟥 Failed jobs : 0
🟨 Partially successful jobs : 0
🟩 Successful jobs : 0

Total data protected : 0
Total media used : 0

Current job activity:

Active jobs : 0
Jobs scheduled for the next 24 hours : 0

Drives

Total drives : 0
🟥 Unusable drives : 0
🟩 Active drives : 0
🟦 Available drives : 0

Services

Total services : 0
🟥 Stopped services : 0
🟨 Paused services : 0
🟩 Running services : 0

Master Servers

Total servers : 1
🟥 Unreachable servers : 0
🟨 Offline servers : 0
🟩 Online servers : 1

Logged in as: [Administrator]

Page generated: [November 11, 2004 9:22:36 AM]

Figure 3: Real-Time alert and notification management consolidation gives users a single health view of their entire environment.

For more in-depth information on the NetBackup Operations Manager, please reference the Management, Alerting and Reporting for VERITAS NetBackup™ 6.0 white paper.

VERITAS NetBackup™ Desktop and Laptop Option

To meet the needs of corporations with desktop and laptop users that have critical data, VERITAS Software introduces the VERITAS NetBackup™ Desktop and Laptop Option. The VERITAS NetBackup Desktop and Laptop Option offers continuous disk-based data protection for users whether they are in the office or on the road. This new NetBackup option enables users to restore their own files and maintain synchronization between multiple desktops and laptops. By automatically copying user data to existing network storage or to the local machine, the NetBackup Desktop and Laptop Option easily integrates into existing IT infrastructure and policies, lowering the total cost of ownership.

The NetBackup Desktop and Laptop Option is a "lightweight" network share based protection and synchronization solution. Users can work and travel with peace of mind, knowing that their data is safe. Whether users require continuous backups, scheduled backups or manual backups the NetBackup Desktop and Laptop Option is able to deliver on flexibility.

Organizations that have multiple desktops can use the NetBackup Desktop and Laptop Option to automatically synchronize data between their computers via a network share so they have the most up-to-date file versions where they need it most, no matter which computer they use. To allow further efficiency, NetBackup Desktop and Laptop Option users can easily retrieve their own data or files through the intuitive user interface whether in the office or on the road.

Because the NetBackup Desktop and Laptop Option has a simple design, a separate, dedicated application server is not required allowing the solution to fit easily into existing infrastructure and comply with company policies already in place. In addition, the NetBackup Desktop and Laptop Option utilizes existing data storage for housing all of the individual user data. This allows a company to adopt a solution for protecting desktops and laptops without additional hardware, personnel or large investments.

DISK BASED BACKUP AND RECOVERY

SYNTHETIC BACKUP

NetBackup software allows users to create synthetic backups. The NetBackup software user needs to create a traditional full backup (non-synthesized) to initiate the process. Once this has been completed, the user will no longer need to create traditional full backups. The NetBackup user will be able to create synthetic full backups from other synthetic full backups (see figure 4 below). NetBackup can also create a synthetic cumulative incremental backup from a cumulative incremental backup plus any number of differential incremental backups if required. A NetBackup client can then use the synthesized backup to restore files and directories in the same way that a user would restore data from a traditional backup.

Benefits of Synthetic Backups

There are several benefits to the NetBackup user by performing synthetics backups. They are as follows:

Processing Takes Place on the NetBackup Master and Media Server(s) Instead of the Client

One advantage of synthesizing a full backup is that the processing of the backup is performed on the NetBackup master/media server and not on the NetBackup client. During a traditional full backup, all files are copied from the NetBackup client to a NetBackup master or media server, even though those files may not have changed since the last incremental backup.

When the NetBackup user creates a synthetic full backup, the NetBackup software takes full advantage of the fact that new or changed files have already been copied to the media server during the last incremental backup. The NetBackup software does not require that the client even be running in order to piece the incrementals together on the media server to form a new, accurate full backup.

Improves Recovery Operations

Synthetic backups empower NetBackup users to restore a client system or data from a single backup image rather than restoring from a series of backup images. This ability significantly increases recovery speed and performance.

Reduce Network Traffic

Another benefit of synthetics backups is that files are transferred over the network only once, reducing network traffic as well as the number of tapes needed to store the data.

Use Drives More Effectively

Backups can be synthesized when drives are not generally in use. For example, if backups occur primarily overnight, the drives can be busy synthesizing full backups during the day.

How Synthetic Backup Works Example

The following figure illustrates an example of the creation of synthetic full backups (B and C) from an existing full backup (A) and the incremental backups between full backups.

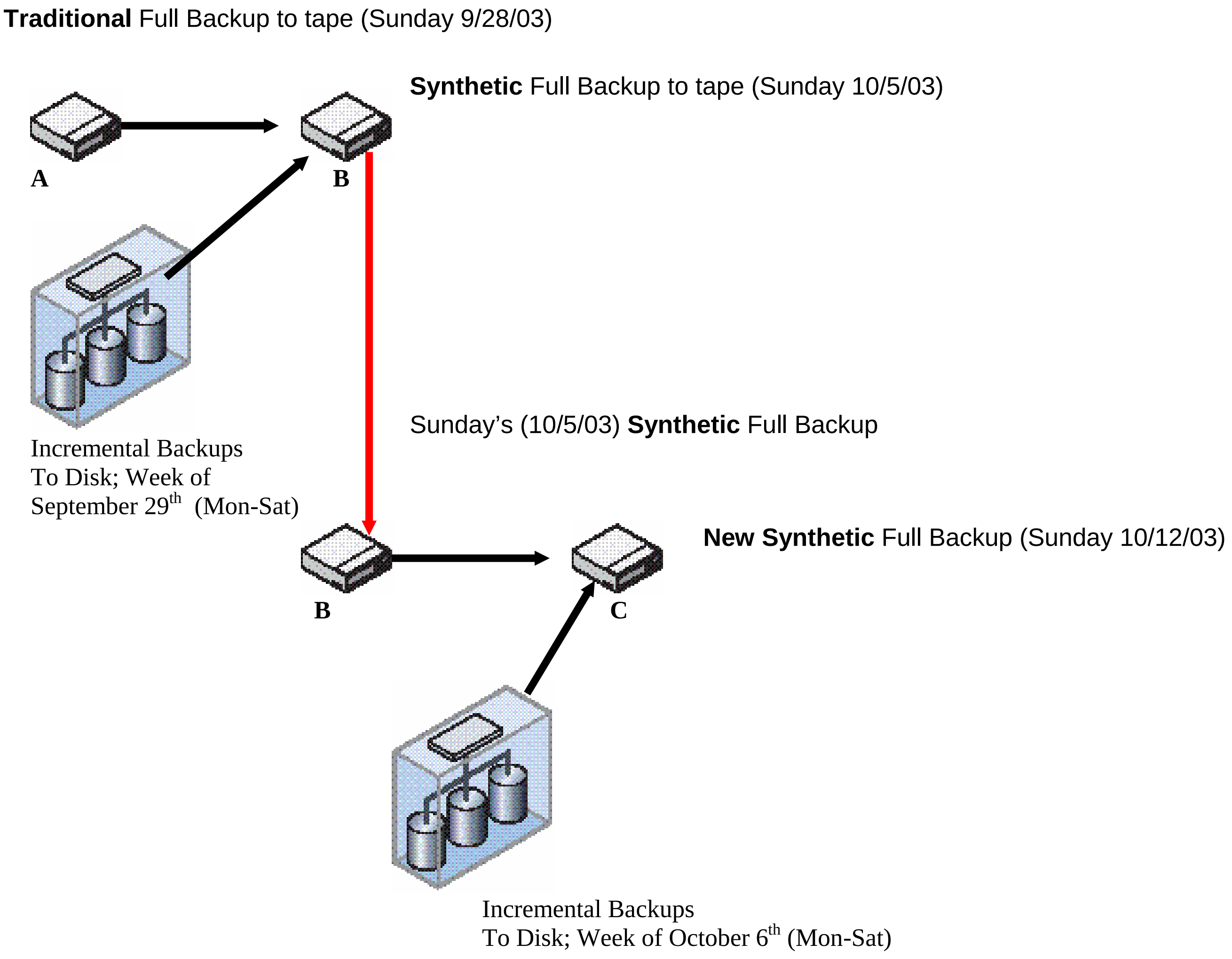

Traditional Full Backup to tape (Sunday 9/28/03)
Synthetic Full Backup to tape (Sunday 10/5/03)
A
B
Incremental Backups To Disk; Week of September 29th (Mon-Sat)
Sunday's (10/5/03) **Synthetic** Full Backup
New Synthetic Full Backup (Sunday 10/12/03)
B
C
Incremental Backups To Disk; Week of October 6th (Mon-Sat)

Figure 4: A NetBackup Synthetic Backup Example

As you can see in the above example, the traditional full backup (A) and the incremental backups are created using the traditional backup method of copying data from the client's file system to the disk staging area and then moving the data to tape to create the synthetic backup image (Synthetic full backups B and C). The synthetic backups do not interact with the client system at all, but are instead synthesized on the NetBackup media server.

Example Scenario in Which a Synthesized Backup Would Be Beneficial

An example of an environment where synthesized backups would be useful would be if the set of NetBackup clients to be backed up experience a moderate to low rate of change in their file systems every day.

If the clients experience a high rate of change daily, the incrementals would be too large and a synthetic backup would not be any more useful than creating a traditional full backup. An example of this situation would be a medical office, where NetBackup clients may contain patient records. The changes to the medical record files are appended and the rate at which new NetBackup clients are added is low.

For additional information on synthetic backup, please refer to the NetBackup Disk Capabilities white paper.

DISK STAGING

Disk Staging provides a backup method for NetBackup administrators to create backup images on disk initially, and then move the images to another media type at a later point in time. NetBackup software's disk staging works by providing a two-stage process for creating NetBackup backup images on disk, and then moving the backup images to another media type at a later, more convenient time. In addition, Disk Staging can facilitate faster backups and restores, and the NetBackup user can use disk staging to facilitate streaming data to tape devices without the drawbacks of multiplexed images.

Disk staging may be appropriate for your NetBackup environment if you are trying to achieve the following objectives:

- To allow backups when tape drives are scarce or unavailable.
- To allow for faster restores from disk.
- To facilitate streaming data to tape without image multiplexing.

How Disk Staging Works

An example of how disk staging works is as follows:

A hypothetical NetBackup customer generates the following amounts of backup data:

Monday:	200MB
Tuesday:	300MB
Wednesday:	300MB
Thursday:	200MB
Friday:	500MB

The hypothetical NetBackup customer decides to perform backups to the disk storage unit daily, and the relocation from the disk storage unit to the final storage unit is performed daily.

The disk staging storage unit this customer must use would have to be at least 500MB, large enough to hold the maximum amount of data that may be generated in one day. If the NetBackup administrator wishes to keep only one day's amount of data on the disk staging storage unit, a 500MB disk staging storage unit would be adequate, assuming that the relocation schedule successfully runs and moves the data to tape daily. The space requirements might have to be adjusted if the administrator wants to keep the data on disk for more than one day.

Disk Staging is conducted in two separate operations:

- Stage I: A backup creates an image on the disk storage unit.
- Stage II: A relocation schedule determines when the image from the disk storage unit should be relocated to the destination storage unit.

The NetBackup disk staging procedure is demonstrated below:

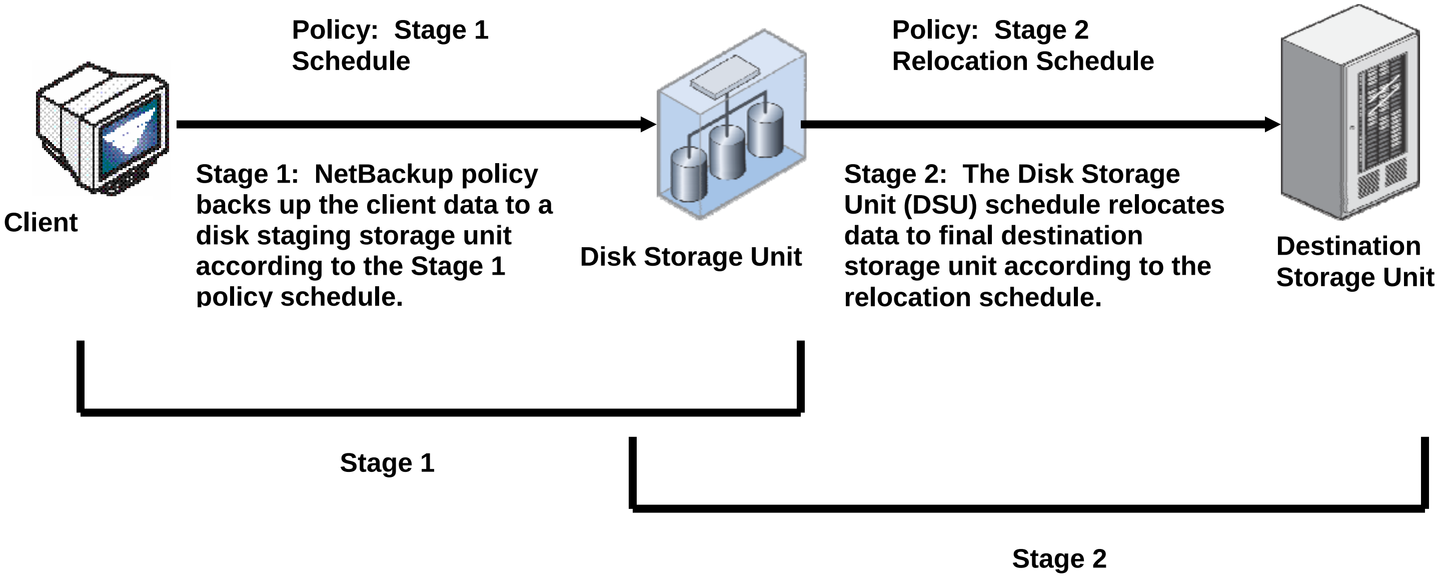

Policy: Stage 1
Schedule
Policy: Stage 2
Relocation Schedule
Client
Stage 1: NetBackup policy backs up the client data to a disk staging storage unit according to the Stage 1 policy schedule.
Disk Storage Unit
Stage 2: The Disk Storage Unit (DSU) schedule relocates data to final destination storage unit according to the relocation schedule.
Destination
Storage Unit
Stage 1
Stage 2

Figure 5: NetBackup Disk Staging Procedure Example

In the first stage of the backup, clients are backed up by a policy that indicates a disk storage unit as the destination storage unit. The schedule for Stage 1 is configured like any other backup.

In the second stage of disk staging, images are relocated from the disk storage unit to the destination storage unit.

The images are relocated based on the relocation schedule configured during setup. This is done by clicking the Disk Staging Schedule button.

For additional information on disk staging, please refer to the NetBackup Disk Capabilities white paper.

New with NetBackup 6.0: NetBackup High and Low Water Mark Settings

NetBackup uses the High Water Mark and Low Water Mark settings to maintain free space on the NetBackup disk staging storage unit.

High Water Marks

The High Water Mark setting is a threshold that, when reached, signals to NetBackup that the disk storage unit should be considered full. The NetBackup default is set at 98%.

NetBackup does not assign a new job to a storage unit that is considered full. Once the capacity of the storage unit is below the High Water Mark, jobs can once again be assigned to the storage unit.

If NetBackup cannot find a storage unit to assign to the job, the job fails. If the storage unit is a disk staging storage unit and the High Water Mark is exceeded while a job is running, the storage unit will begin to expire images as needed to accommodate the backup data.

Low Water Marks

The Low Water Mark pertains only to disk storage units acting as temporary staging storage units. The NetBackup default value is set at 80%.

Once the High Water Mark is reached, space is created on the disk storage unit until the Low Water Mark is met. To do this, NetBackup may copy the images to other storage units, or expire the images (oldest first) to free space. The Low Water Mark setting cannot be greater than the High Water Mark setting.

If the Low Water Mark and the High Water Mark are set to the same value, NetBackup expires only two images.

NETBACKUP AND NETWORK APPLIANCE INTEGRATION

NEARSTORE DISK STORAGE UNIT

NetBackup 6.0 introduces the Network Appliance (NetApp) NearStore disk storage unit.

Essentially, NetBackup writes client backup data to NearStore disk in tar format. After the tar image is complete, a snapshot is taken of the tar image and the data is converted into a WAFL qtree on the NearStore machine.

Useful terms to understand when configuring a NetBackup NearStore disk storage unit are as follows:

- WAFL (Write Anywhere File Layout): The file system used in all Network Appliance storage servers. WAFL supports snapshot creation.
- qtree (quota tree): A subdirectory in a NearStore volume that acts as a virtual subvolume with special attributes, primarily quotas and permissions.
- Snapshot: A read-only, point-in-time copy of the entire volume. A snapshot captures file modifications without duplicating file contents.

Advantages of the NearStore Storage Unit

Key advantages of the NetBackup NearStore Storage Unit are as follows:

- Innovative NetBackup and NearStore Environment Integration
  Client backups to a NearStore storage unit involves the media server providing metadata that allows the NearStore to convert the tar image into the WAFL format.

  To restore files from a NearStore storage unit (Data ONTAP 7.1.1), NetBackup clients are able to directly NFS/CIFS mount the WAFL qtree and restore the backup images. The Backup, Archive, and Restore client interface can also be used. (Please note, it is required for restoring images when Data ONTAP 7.1 is used.).

- Single Instance Storage
  NearStore avoids duplicating disk blocks by comparing the latest snapshot with the active file system. A snapshot does not consume disk space unless blocks in the active file system being snapped are modified or removed.

- o Uses point-in-time snapshot
  The snapshot that NearStore creates is a point-in-time snapshot.

An example of a NetBackup and Network Appliance NearStore environment is shown in figure 6 below.

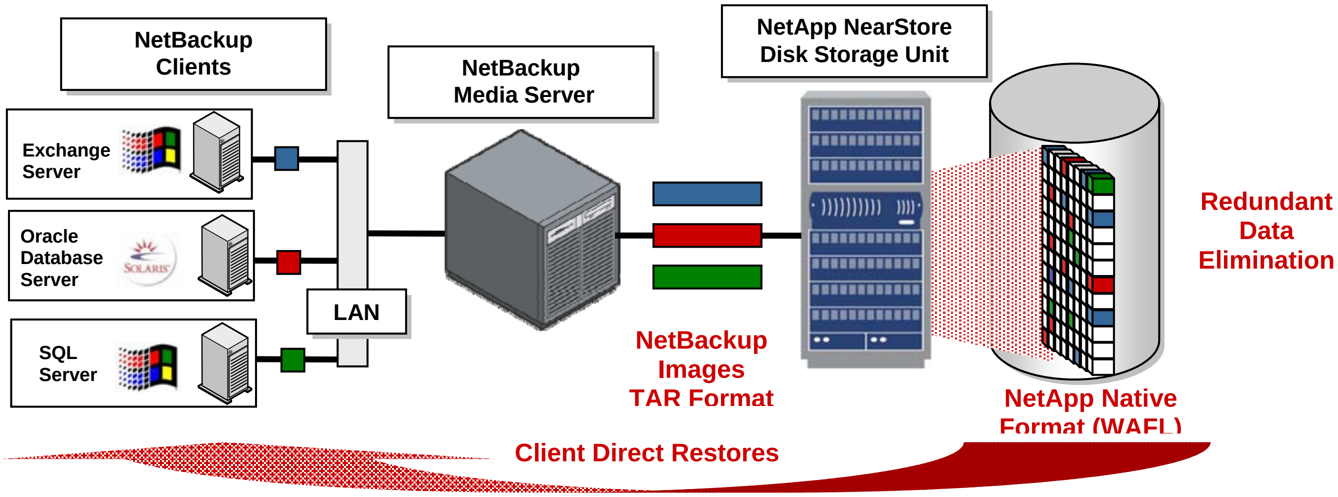


Figure 6: NetBackup and NearStore example

For additional information on how to configure NetBackup NearStore disk storage units, please reference the NetBackup System Administrator Guide.

SNAPVAULT DISK STORAGE UNIT

In addition to making a snapshot of client data on the NAS host, NetBackup can now copy the NAS snapshot data to a disk-based SnapVault secondary host for additional security, remote office backup convenience and speed of restore. In this case, the NAS filer containing the NAS snapshot is the primary host, and the SnapVault server containing a disk backup of the snapshot is the secondary host. SnapVault backups can be made at frequent intervals, and can be retained on disk as long as desired.

SnapVault is discussed in more detail in the Advanced Client section of this white paper below starting on page 25.

For additional information, please reference the NetBackup/NetApp Integrated NAS Protection and the NetBackup/NetApp Optimized Disk-Based Data Protection white papers.

CHECKPOINT RESTART FOR BACKUP AND RECOVERY

Checkpoint Restart allows a failed backup or recovery job to be resumed from the last checkpoint. Checkpoints are taken periodically during a backup or a recovery. Therefore, if a backup or recovery job fails, the issue causing the failure can be corrected and the job can be resumed from the last checkpoint rather than at the beginning of the backup or recovery job. The result is a significant savings of time and resources. In addition, an active backup or recovery job may be suspended and then resumed from the last checkpoint at a later time. This allows administrators to suspend backups and recoveries if necessary to prioritize more important backup and recovery jobs and operations.

Checkpoint Restart for backup and recovery is supported for the following:

- Backup and recovery jobs
- Resume on file boundaries. This means the backup or recovery is resumed from the next file after the last check-pointed file. A resume cannot occur within a file.
- Backups and recoveries of file-system backups (i.e. backups and recoveries which use the NetBackup Standard or NetBackup Microsoft Windows policy types only).
- File system local and alternate client snapshot backups and recoveries
    - Backup: File system local and alternate client snapshot backups are supported. However, other off-host backup methods (e.g. Media Server Copy or Third Party Copy) are not supported.
    - Recovery: Third Party Copy and Media Server Copy images that use Standard policy types are supported for recoveries, but cannot use the suspend/resume functionality if the backup image has changed blocks. The FlashBackup method is not supported.

An example of NetBackup software's Checkpoint Restart functionality is demonstrated in Figure 7 below:

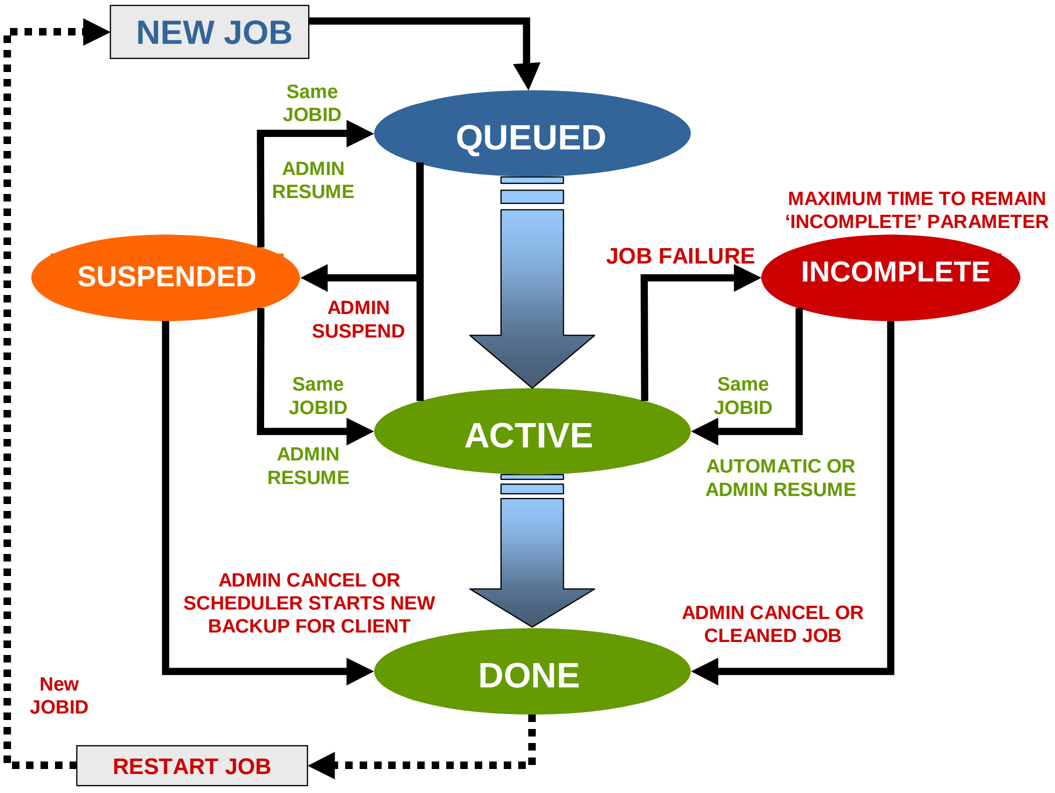

NEW JOB
Same JOBID
QUEUED
ADMIN RESUME
MAXIMUM TIME TO REMAIN 'INCOMPLETE' PARAMETER
JOB FAILURE
SUSPENDED
INCOMPLETE
ADMIN SUSPEND
Same JOBID
Same JOBID
ACTIVE
ADMIN RESUME
AUTOMATIC OR ADMIN RESUME
ADMIN CANCEL OR SCHEDULER STARTS NEW BACKUP FOR CLIENT
ADMIN CANCEL OR CLEANED JOB
DONE
New JOBID
RESTART JOB

Figure 7: Example of NetBackup software's Checkpoint Restart functionality

THE NETBACKUP ADVANCED CLIENT

The NetBackup Advanced Client brings together as a single licensed package a diverse set of advanced backup and recovery methods to provide a comprehensive approach to snapshot data in support of backup and recovery operations. These methods enable a customer to tailor the backup and restore performance to obtain one or more of the following benefits:

- Faster restores
- Faster backups
- Lower-impact backups

The NetBackup Advanced Client is designed to make it much easier for the NetBackup user to configure and use the advanced backup and recovery methods available with this product. The following backup and recovery methods that have been combined into the new NetBackup Advanced Client are as follows:

- Local Snapshot
- FlashBackup
- Instant Recovery
- Block Level Incremental (BLI) Backup and Recovery
- Off-Host (ServerFree) backup
  - → Alternate Client
  - → Media Server Copy
  - → Third-Party Copy
  - → Array Support
- Network Attached Storage (NAS)
  - → Support for Network Appliance SnapVault, Snapshot and SnapRestore

What's New with NetBackup 6.0?

Key new Advanced Client features available with NetBackup 6.0 are as follows:

- Network Appliance SnapVault
- Support for Disk Array Snapshots on Windows
- Snapshot Policy Configuration Wizard
- Instant Recovery Enhancements

Disk-Based Snapshot Features Overview

A snapshot is a disk image of the client's data that is created almost instantaneously. NetBackup software backs up the data from the snapshot image, not directly from the client's primary disk. Snapshots of data allow client operations and user access to continue without interruption during the backup process.

A snapshot image is required for all features of the Advanced Client. A number of methods are provided for creating snapshots. The NetBackup user can select the snapshot method manually from the Policy dialog of the NetBackup Administration Console, or allow NetBackup software to select the preferred snapshot method that should be used.

THE NETBACKUP ADVANCED CLIENT AND ONLINE FILE SYSTEM BACKUPS

Local Snapshot Method

This basic snapshot method produces a snapshot that can be backed up to any NetBackup media server. The following diagram below shows a network configuration for a local backup of a snapshot. The network configuration is identical to that for normal NetBackup operations. The difference is a snapshot is first created at a point-in-time and moved to the media server rather than using a traditional file by file approach.

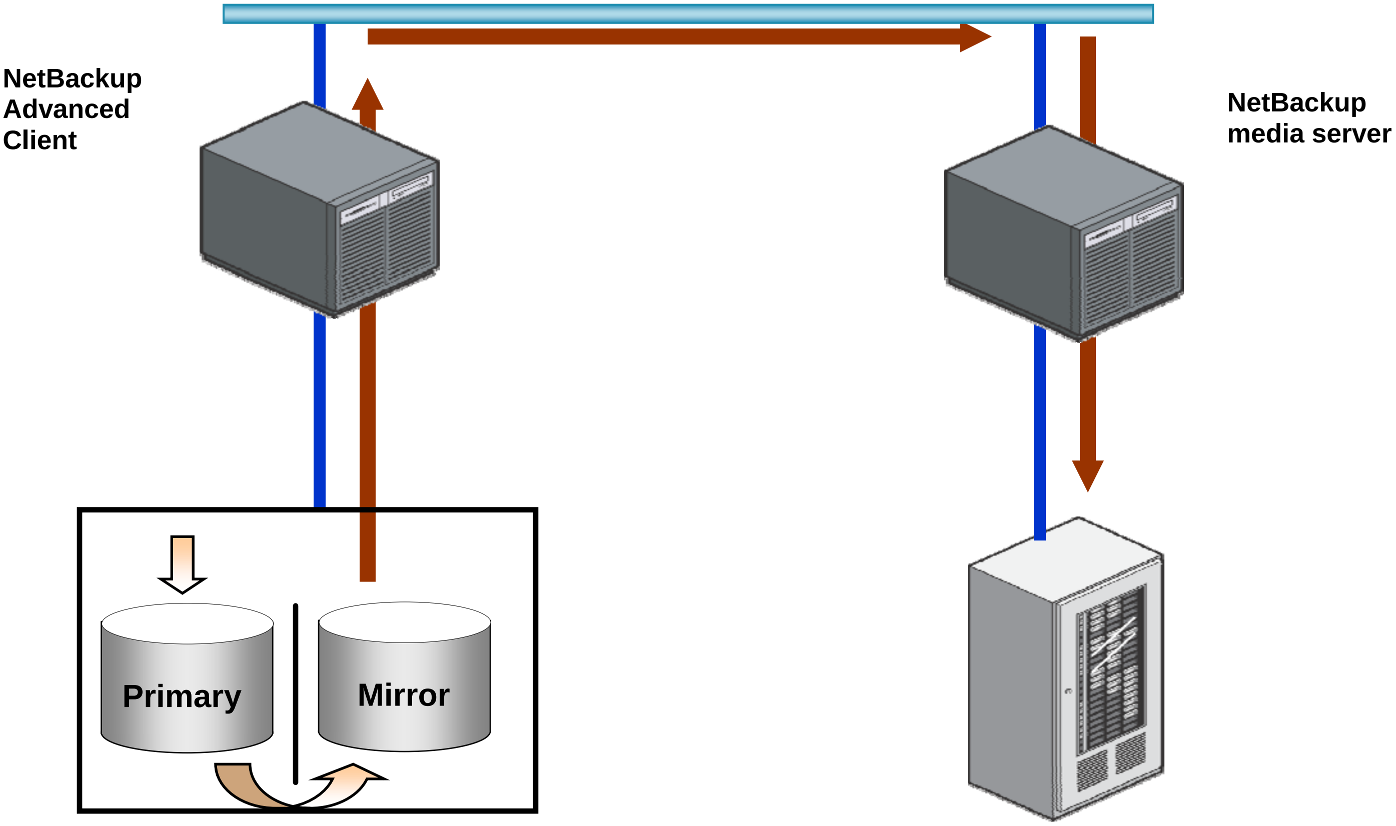


Figure 8: NetBackup Advanced Client performs a local snapshot backup

FlashBackup Method

While your critical enterprise server is up and running and performing its primary function, the NetBackup Advanced Client allows the user to use the FlashBackup method to create lightning-fast backups in a fraction of the time required by conventional backup methods, while still providing data integrity and individual file restorability.

The FlashBackup method uses snapshot technology to provide high performance, online “file image” backups of mounted file systems[1] while still allowing restores of individual files and directories. The FlashBackup method significantly enhances backup performance for file servers, web servers, and Internet mail servers that have file systems, which contain a large number of small files. High performance backups are accomplished with minimal overhead on the host system being backed up. The FlashBackup method delivers the performance of raw file system backup without losing the flexibility of restores at the individual file and/or directory level. This snapshot method can also be used with either disk or tape storage units.

[1] Support for Sun Solaris, HP-UX and Windows operating systems.

Both full and incremental FlashBackup method backups are supported and are performed with a single sweep of the source disk, eliminating unnecessary head movement. All restores (i.e. from tape) are performed with a single pass of the media, which optimizes restore times.

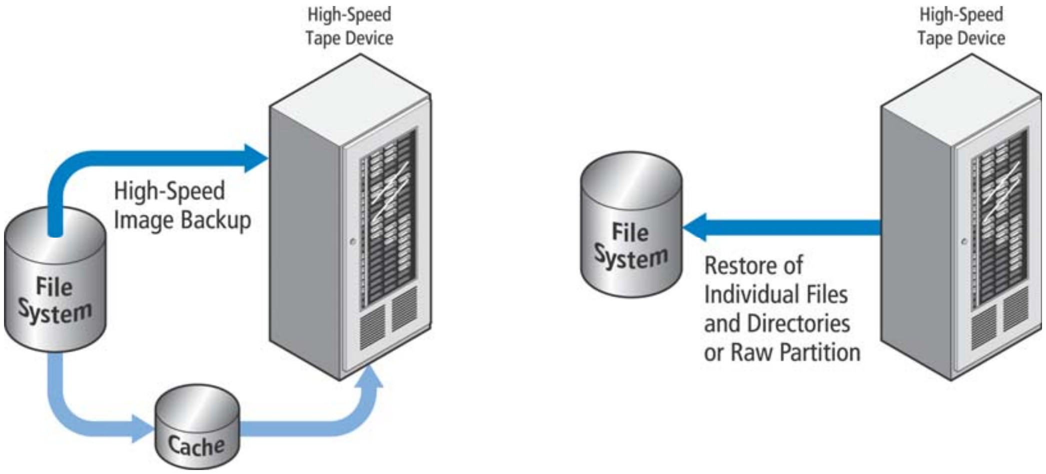


Figure 9: The NetBackup Advanced Client FlashBackup Method

Figure 9 above illustrates the FlashBackup method backup and recovery process. The FlashBackup method delivers the high performance of a raw partition backup since it bypasses the buffered I/O of the file system and dramatically reduces CPU utilization during the backup process. A disk "snapshot" capability provides a consistent view of the live disk during backup. This provides a point-in-time backup of the disk, even though users may continue to change the contents of the disk during the backup operation. The FlashBackup method also allows NetBackup software to recover individual files, directories or raw partitions, so that customers do not have to sacrifice granularity for performance.

The FlashBackup method can dramatically enhance backup performance — especially in environments with large numbers of small files. Backup performance improvements of 6x –10x are commonplace in NFS file server, web server, and Post Office Protocol (POP) mail server environments. For example, Figure 10 below graphs backup times for a customer with a large number of files on their file system that reduced their backup window from 72 hours using a standard backup to 11 hours using the FlashBackup method.

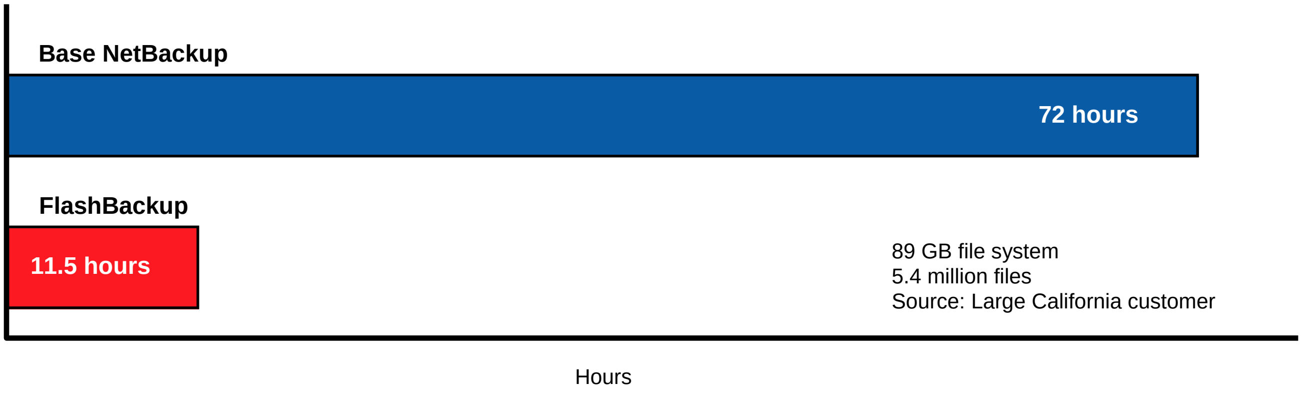


Figure 10: Performance improvements using the Advanced Client's FlashBackup Method

The Advanced Client FlashBackup method is available on HP-UX, Sun Solaris and Windows.

THE NETBACKUP ADVANCED CLIENT AND DISK ARRAY SUPPORT

For many of today's largest enterprises that are using disk arrays, traditional backup methods simply do not suffice. Data availability must be kept at a maximum, while backup impact to production systems must be kept at a minimum. Leading storage manufacturers have developed innovative data snapshot methods, and when combined with a backup and recovery application strive to address these challenges. The NetBackup Advanced Client provides a snapshotting method specifically designed for disk arrays that enables NetBackup software to exploit these popular hardware data snapshot techniques.

In most cases, a third mirror of the data is created within a disk array to serve as the backup object. The Advanced Client splits the third mirror away from the primary mirror and secondary mirror to prepare the data for backup. NetBackup then performs the backup, sending the data traffic to a NetBackup server, which processes the data to a tape device. The Advanced Client may also use the Off Host backup method to move the backup data directly from disk to tape. When the backup is complete, the NetBackup software establishes synchronization between the third mirror and the primary mirror for data consistency. This can be done immediately or at the time of the next backup.

New! NetBackup 6.0 Advanced Client now supports disk array snapshots on Windows.

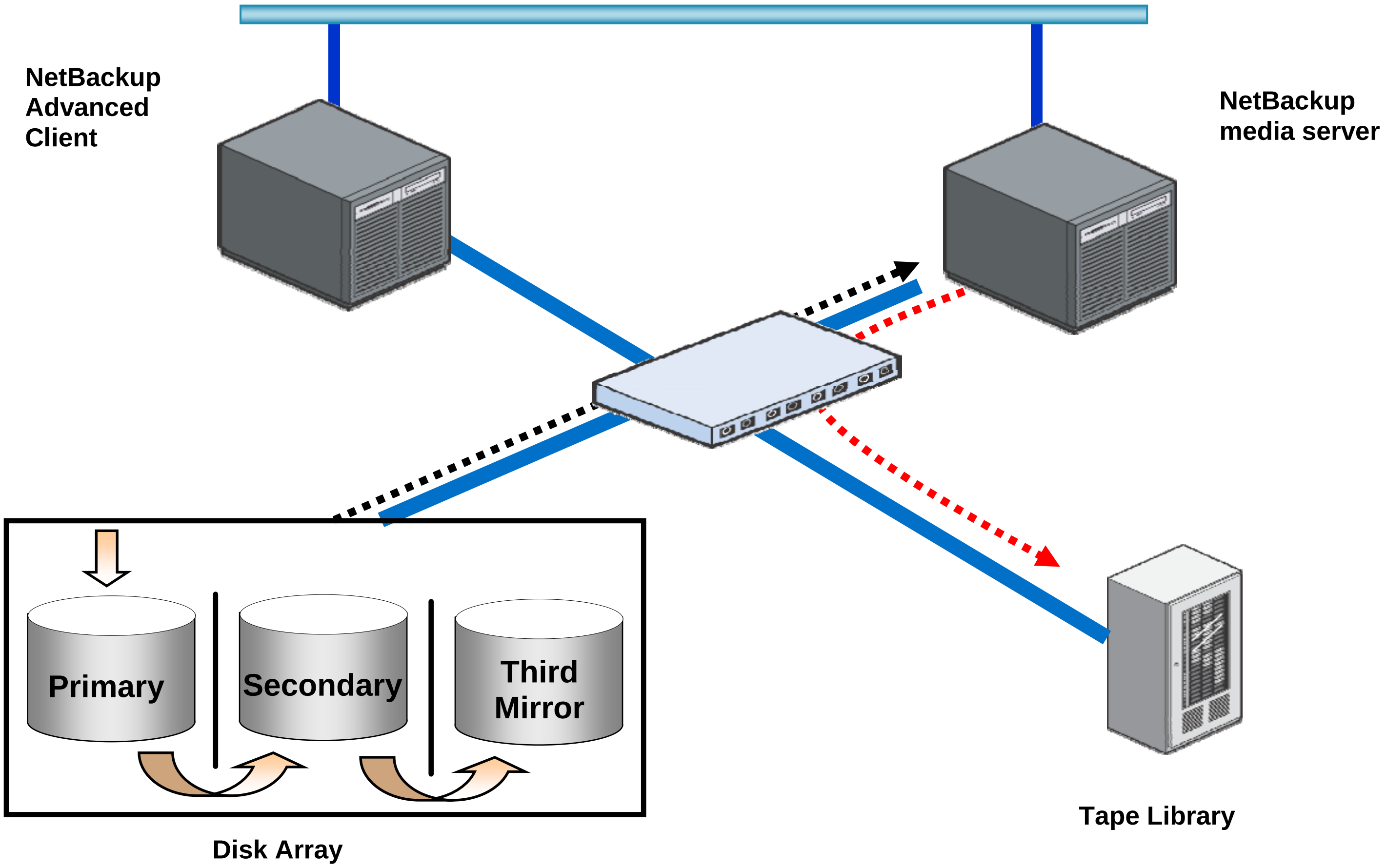


Figure 11: NetBackup Advanced Client performing a split mirror backup

In Figure 11 above, the Advanced Client is using the alternate client backup capability, which is discussed in more detail below. The third-mirror is mounted on another host in this scenario the NetBackup media server. The dotted black line demonstrated this functionality. The data is then backed up to tape. The dotted red line shows the data movement to tape. The NetBackup Advanced Client machine being backed up is no longer impacted during this off-host backup operation. The Advanced Client can also be configured to move data from the disk array across the LAN to tape. In this scenario, the third mirror would be mounted on the Advanced Client and backed up through the NetBackup media server.

The Advanced Client supports the following third-party disk array snapshot methods:

- HP StorageWorks Business Copy XP
- EMC TimeFinder
- EMC Clariion
- Hitachi Data Systems ShadowImage
- Sun StorEdge ShadowImage

THE NETBACKUP ADVANCED CLIENT AND INSTANT RECOVERY

NetBackup software is able to retrieve point-in-time copies from disk to produce the fastest recovery possible. By using the Advanced Client, backup administrators can now combat end user error and application corruption quicker than ever before.

The point-in-time copy capabilities of the Advanced Client allow users to select the method that makes the most sense for their environment. For example, users can select the volume snapshot feature of the VERITAS Volume Manager if this is the snapshot method that will meet the backup and recovery requirements of their environment. With all of the snapshot methods available with the Advanced Client, the end result is the ability to capture data at the client without moving data across the network or to tape. Only catalog entries are sent to the NetBackup master server to accurately track the point-in-time copy that was created or identified for use with the NetBackup software.

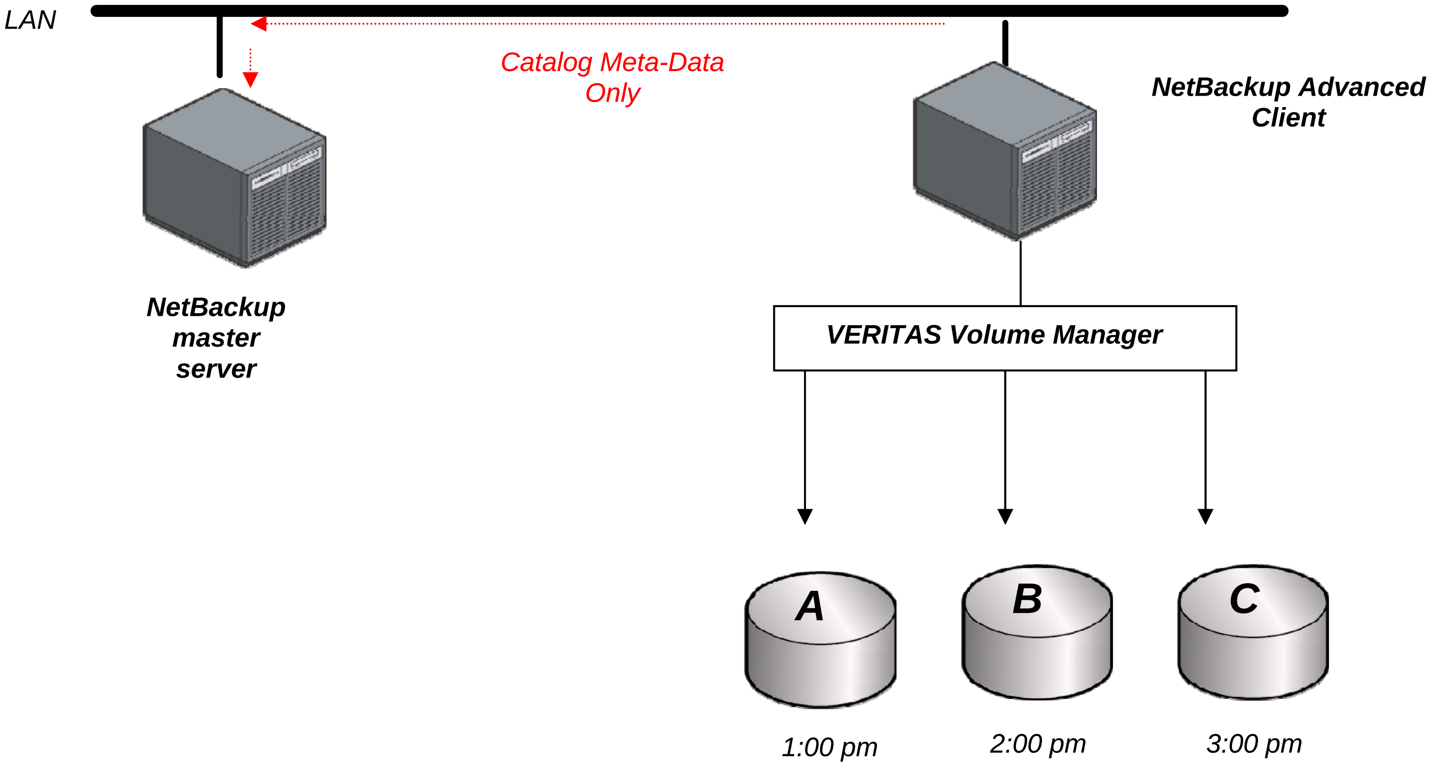


Figure 12: The VERITAS Advanced Client and the Instant Backup and Recovery Method

The NetBackup Advanced Client Instant Recovery supported snapshot methods are VERITAS Storage Foundation Suite products (i.e. VERITAS File System, VERITAS Volume Manager or VERITAS Volume Replicator), SFW Fast File Resync, and also Network Appliance snapshot integration. The Instant Recovery method is supported for use with Oracle, SQL and DB2 databases. For up to date NetBackup 6.0 support requirements, please go to http://support.veritas.com/ .

NETBACKUP ADVANCED CLIENT AND OFF HOST BACKUP

The principal goal of the NetBackup Advanced Client and off-host backup is to move the I/O processing off the primary NetBackup client (i.e. application host) to a backup agent. The NetBackup Advanced Client has three different methods to perform off host backups:

- **Alternate Client Backup**: The backup is performed by another client in a split mirror or data replication configuration.
- **NetBackup Media Server**: The backup is performed by a NetBackup media server.
- **Third-Party Copy Device**: the backup is performed by an independent backup agent that uses the Extended Copy command.
- **NEW! Support for Microsoft Exchange** —NetBackup can reduce backup impact and improve performance by performing an off-host backup of Microsoft Exchange server.
- **NEW! Support for AIX and Linux** — Off-host backups that reduce backup impact can now be performed on the AIX and Linux platforms.

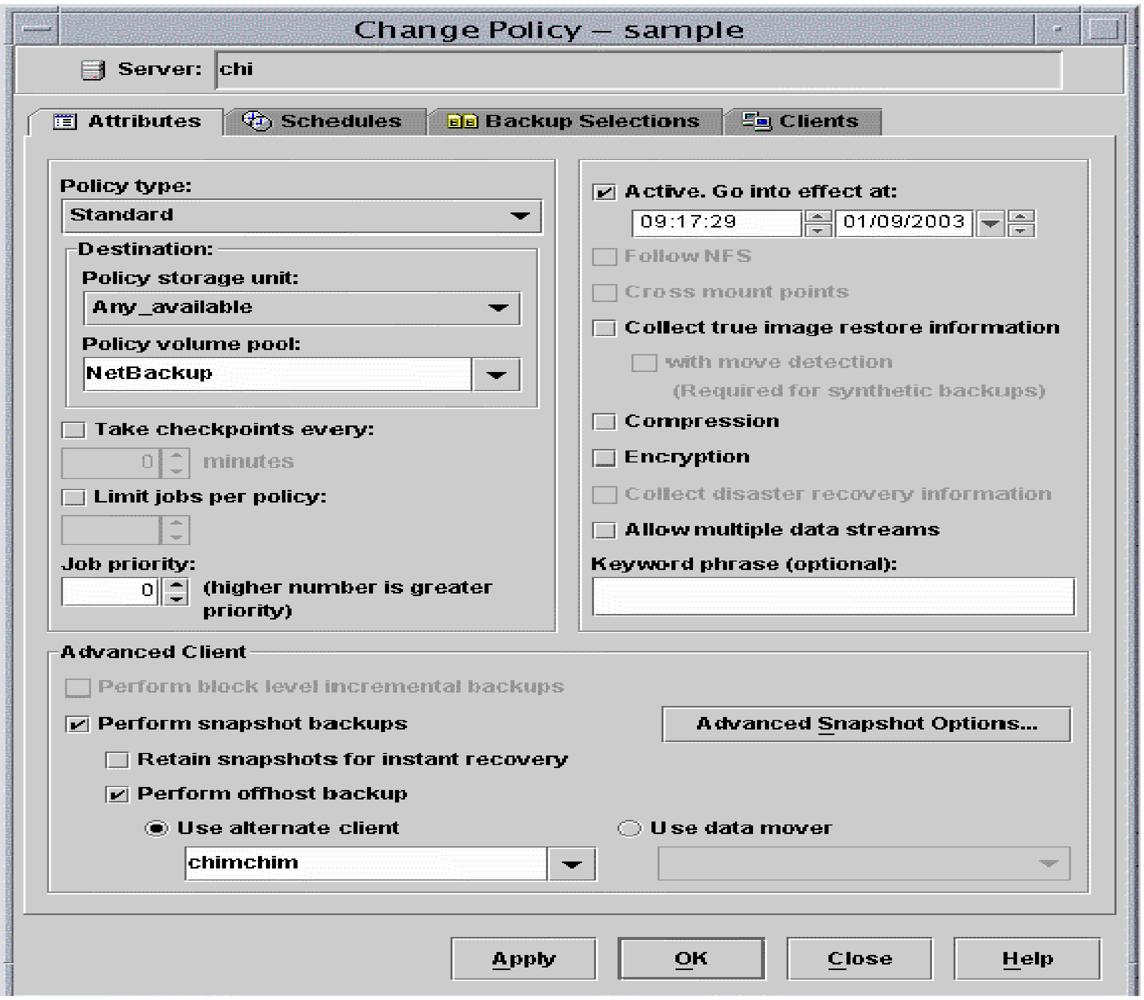
Alternate Client Backup Method

The Alternate Client Backup Method off-loads the backup processing to another client machine. Offloading the work to another or “alternate” client machine saves computing resources on the original client machine. The snapshot is created on the alternate client, and the backup has zero impact on the original client.

The Alternate Client backup method uses a NetBackup master server, which is connected to two clients and a NetBackup media server. The primary or original NetBackup client contains the data to be backed up, and the alternate NetBackup client has a copy of that data. The NetBackup media server can be accessed by the alternate client. The result is that the NetBackup media server can back up the alternate client as a local host.

Figure 13 below shows and example of how to configure a NetBackup policy to perform an Advanced Client off-host alternate client backup.

The NetBackup Advanced Client’s Alternate backup method supports Oracle, DB2 and Microsoft SQL Server databases.



Server: chi

Policy type: Standard

Destination:

Policy storage unit: Any_available

Policy volume pool: NetBackup

□ Take checkpoints every: 0 minutes

□ Limit jobs per policy:

Job priority: 0 (higher number is greater priority)

☑ Active. Go into effect at: 09:17:29 01/09/2003

□ Follow NFS

□ Cross mount points

□ Collect true image restore information

□ with move detection (Required for synthetic backups)

□ Compression

□ Encryption

□ Collect disaster recovery information

□ Allow multiple data streams

Keyword phrase (optional):

Advanced Client

□ Perform block level incremental backups

☑ Perform snapshot backups

□ Retain snapshots for instant recovery

☑ Perform offhost backup

● Use alternate client: chimchim

○ Use data mover

Figure 13: Configuring a NetBackup policy to perform an Advanced Client off-host alternate client backup

Third-Party Copy Device and NetBackup Media Server Methods

The NetBackup Advanced Client provides off host backup using snapshot, mapping and third party copy data movement technologies. This technology removes the backup workload from the NetBackup Advanced Client server onto a separate backup agent (e.g. alternate client, NetBackup media server or third-party copy device). Since the overhead is taken off of the client machine during the backup process, performance is significantly improved for the user of the client machine during the backup.

The VERITAS NetBackup Advanced Client and the off host backup method consists of three steps which are described and shown in Figure 14 below:

Step 1. Data Snapshot — VERITAS NetBackup software must create a point-in-time snapshot of the data to perform backups efficiently without an application or database server. The first step in the frozen image or snapshot creation process is to pause the application or database briefly by placing the client machine into backup mode. This process flushes all buffers and makes sure the data is constant at a known point in time. Once this point has been established, a snapshot backup can be engaged using the NetBackup Advanced Client's functionality. Multiple snapshot methods give users an unparalleled level of flexibility.

Step 2. Logical Disk Object Mapping — The underlying technology layer between a snapshot and server-free data movement is logical disk object mapping. VERITAS Software has developed this technology because it is crucial that the data is reliably mapped so its physical location is known. After the snapshot has been taken, the Advanced Client maps the data by drilling down through the I/O stack and linking the logical file names to the actual physical blocks of data. In the event of file system reorganization, sector slippage or RAID 5 degraded performance; the data can be remapped to make sure its integrity is preserved. This technology layer is essential for off-host/server-free data movement. Without it, the potential of data corruption is significant when data needs to be restored to the server. Once the mapping (block list) is completed, it can be sent to the third-party copy engine.

Step 3. True Off Host Data Movement — When the snapshot and mapping operations are completed, the data is ready to be moved by the SCSI Extended Copy Command[2] that can reside in either a Storage Area Network (SAN) hardware device or even on a VERITAS NetBackup media server. In either architecture, the data is no longer moved by the application or database server, but rather offloaded to a third party, either a SAN hardware device or the NetBackup media server. The SCSI Extended Copy engine handles the actual movement of backup data directly from disk to tape in a SAN.

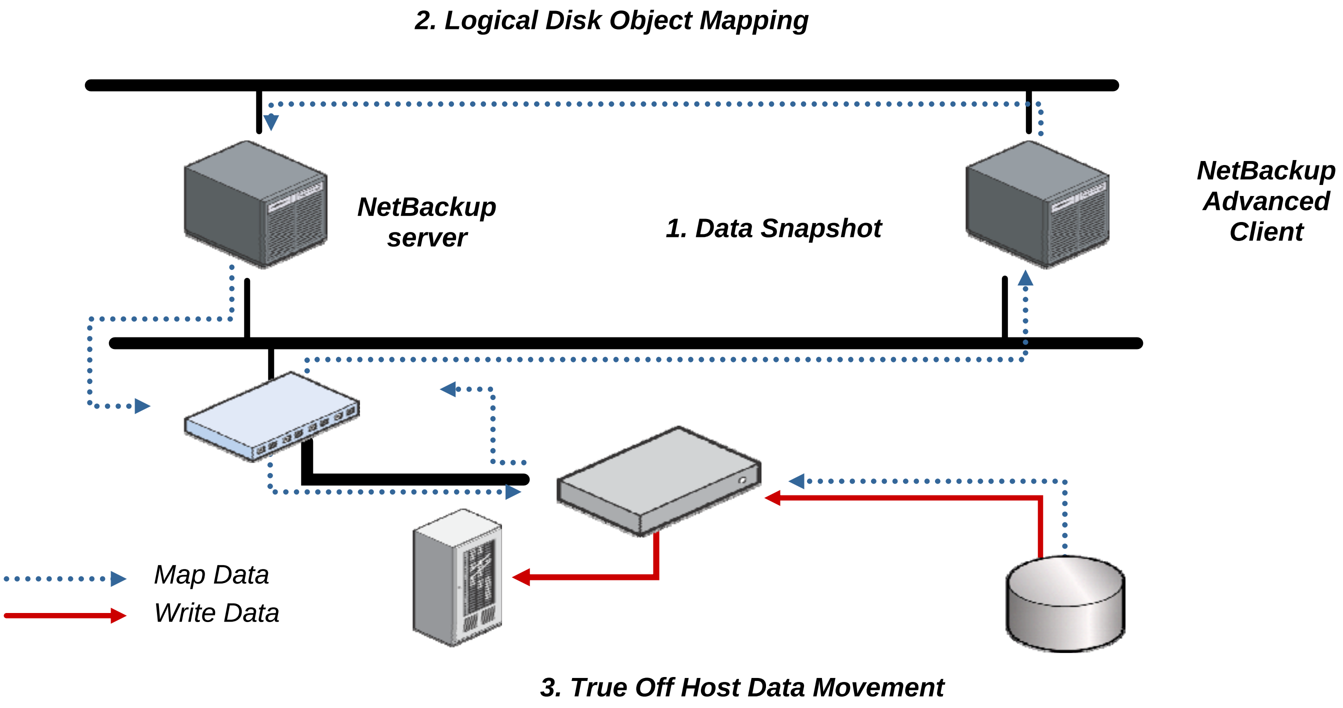

2. Logical Disk Object Mapping
NetBackup server
1. Data Snapshot
NetBackup Advanced Client
Map Data
Write Data
3. True Off Host Data Movement

Figure 14: The NetBackup Advanced Client and the Three Step Off Host Backup Process

The Third-Party Copy Device and NetBackup media server backup methods are supported on HP-UX and Sun Solaris.

[2] The SCSI Copy Command is a block-oriented command that provides device-to-device data movement.

NETBACKUP ADVANCED CLIENT AND BLOCK LEVEL INCREMENTAL BACKUP AND RECOVERY

The NetBackup Advanced Client and its Block Level Incremental Backup and Recovery method is discussed below starting on page 27.

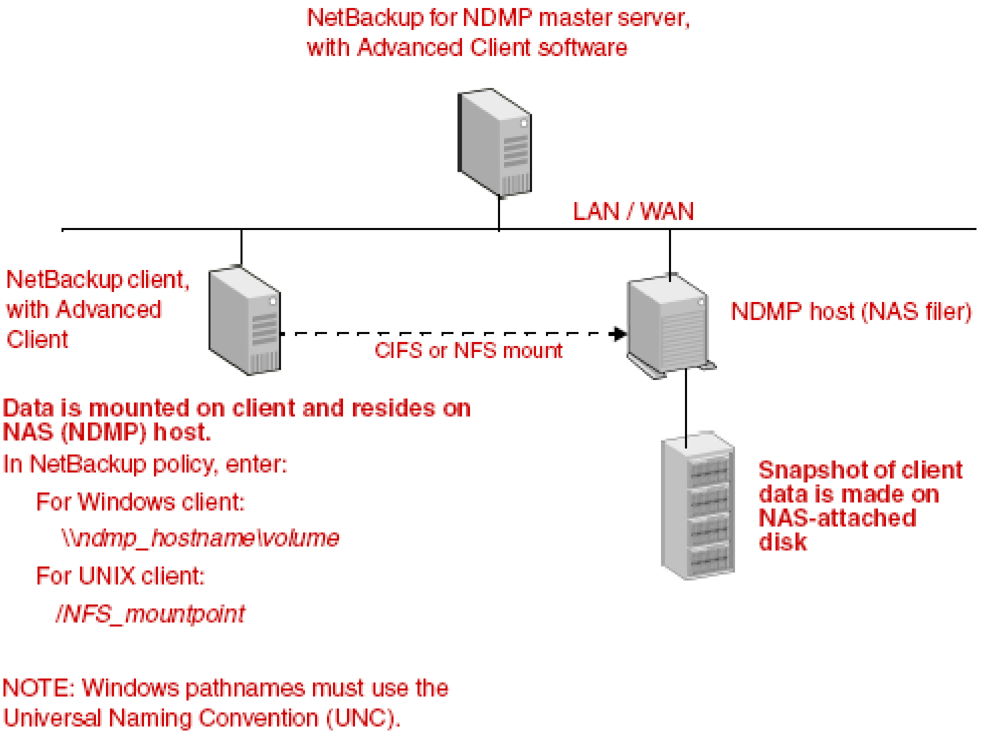
NETBACKUP ADVANCED CLIENT AND NAS SUPPORT

VERITAS Software and Network Appliance have teamed up to deliver a new set of integrated data protection solutions for both NAS and heterogeneous server environments. Organizations can now simplify their data protection strategy by managing all data protection stages from a single interface, including snapshot management for short-term protection and instant recovery, disk-to-disk backups for near-term protection, and NDMP tape backups for long-term storage. The NetBackup 6.0 release introduces a number of innovative solutions that include NDMP enhancements and integration with Network Appliance's Snapshot, SnapRestore, and SnapVault technologies.

NAS SNAPSHOT OVERVIEW

By means of the snapshot feature of Advanced Client and the NetBackup for NDMP option, NetBackup can create snapshots of client data on a NAS (NDMP) host. The client data must reside on the NAS host and be mounted on the client by means of NFS on UNIX or CIFS on Windows.

A NAS snapshot is a point-in-time disk image. NAS snapshots can be retained on disk as long as desired. The data can be efficiently restored from disk by means of the Advanced Client Instant Recovery method. This is shown in Figure 15 below.


NetBackup for NDMP master server, with Advanced Client software
LAN / WAN
NetBackup client, with Advanced Client
CIFS or NFS mount
NDMP host (NAS filer)
Snapshot of client data is made on NAS-attached disk

Data is mounted on client and resides on NAS (NDMP) host.

In NetBackup policy, enter:

For Windows client:

\\ndmp_hostname\volume

For UNIX client:

/NFS_mountpoint

NOTE: Windows pathnames must use the Universal Naming Convention (UNC).

Figure 15: NetBackup and a NDMP snapshot environment

NetBackup creates snapshots on the NAS-attached disk only, and not on storage devices attached to the NetBackup server or the client.

NETBACKUP AND NETWORK APPLIANCE SNAPVAULT

In addition to making a snapshot of client data on the NAS host, NetBackup can also copy the NAS snapshot data to a disk-based Network Appliance SnapVault secondary host for additional security and speed of restore. In this case, the NAS filer containing the NAS snapshot is the primary host, and the SnapVault server containing a disk backup of the snapshot is the secondary host. SnapVault backups can be made at frequent intervals and retained on disk as long as desired.

This is shown in Figure 16 below:

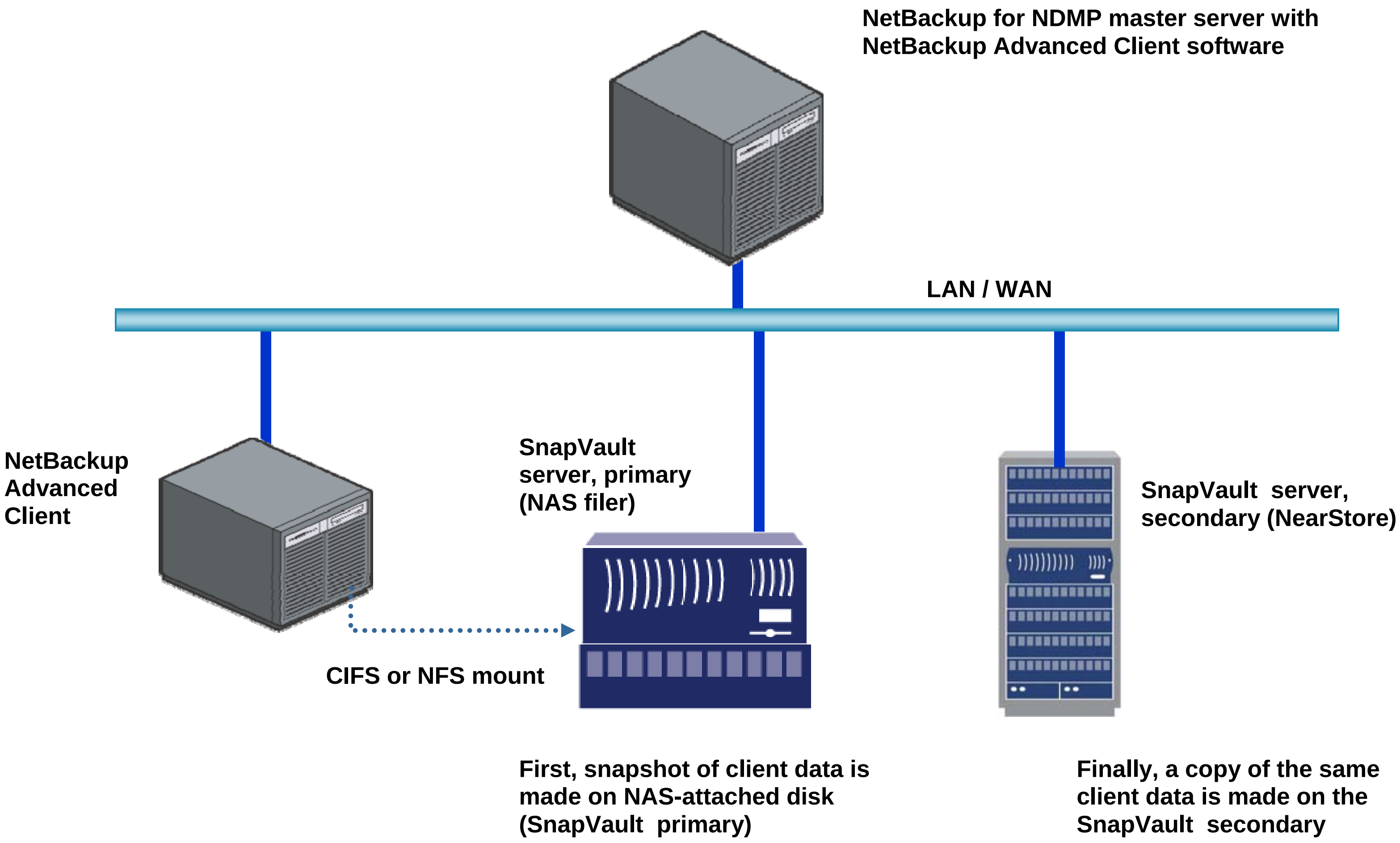

NetBackup for NDMP master server with NetBackup Advanced Client software
LAN / WAN
NetBackup Advanced Client
SnapVault server, primary (NAS filer)
SnapVault server, secondary (NearStore)
CIFS or NFS mount
First, snapshot of client data is made on NAS-attached disk (SnapVault primary)
Finally, a copy of the same client data is made on the SnapVault secondary

Figure 16: NetBackup and Network Appliance SnapVault overview

Network Appliance and VERITAS bring years of collaboration and expertise to the task of offering industry-leading integration of disk and data protection. Their relationship benefits customers with innovative solutions and outstanding cooperative service and support. The two companies have undertaken a full year joint development to deliver their unique disk-based data protection integration. For additional information on NetBackup support and integration for Network Appliance technology, please reference the white papers available on both VERITAS and Network Appliances respective web sites.

For additional information, please reference the NetBackup/NetApp Integrated NAS Protection and the NetBackup/NetApp Optimized Disk-Based Data Protection white papers.

ADDITIONAL INFORMATION ON THE NETBACKUP ADVANCED CLIENT

For additional information on the NetBackup 6.0 Advanced Client, please reference the NetBackup Advanced Client Overview white paper located at www.veritas.com and VNET.

CONTINUOUS DATA AVAILABILITY FEATURES

Timely access to critical data is often the difference between the success or failure of a business. Data must be available to users when they need it. In today's global economy, critical files and databases must often be available 24 hours per day. If access to a critical system is interrupted for any reason, alternative systems must be able to take over the load automatically and transparently. Disaster recovery capabilities must be available so that if the worst happens and a site is completely disabled, critical data can be restored and available online in a few minutes or, in a worst case scenario, a few hours.

VERITAS NetBackup software can be an effective way to provide cost effective disaster recovery protection for mission critical data. NetBackup software delivers online high performance backups of database, file system, and application-specific data, with minimal impact on users or applications. In addition to fast backups, NetBackup software also provides many methods to recover data quickly. VERITAS NetBackup software is an industry leader in providing continuous data availability for all types of mission critical data during backup operations.

ONLINE BACKUPS OF RELATIONAL DATABASE MANAGEMENT SYSTEMS (RDBMS)

NetBackup offers completely online, highly reliable backup solutions for all major databases, including Oracle, IBM DB2 Universal Database, SAP NetWeaver, Microsoft SQL Server, Microsoft Exchange Server, Microsoft SharePoint Portal Server, Lotus Notes & Domino Server, Sybase, and Informix. With these database solutions, online backups for other major applications such as PeopleSoft, Baan, and SAS are enabled. Oracle, DB2, SQL, Exchange, Lotus Notes, SAP NetWeaver, Sybase, and Informix database backups can also be encrypted to enhance security. No matter what the application or environment, NetBackup ensures continuous data availability and complete data protection.

Microsoft SQL Server
Microsoft Exchange Server
Microsoft SharePoint Portal Server

Lotus Notes & Domino Server R5

SAP NetWeaver

IBM DB2 UDB

Database backup performance is critical to data availability, even in online database backup configurations. The NetBackup architecture enables multiple parallel data streams to be pushed to a NetBackup server on the local machine or across the network (see Figure 17 below). On systems where backup media transfer rates far exceed disk or network transfer rates, data streams from multiple disks and clients can be combined into a single stream to drive the offline media at its peak rates — this facility is called multiplexing. Performance scales in a nearly linear manner as additional peripheral devices and backup servers are added incrementally.

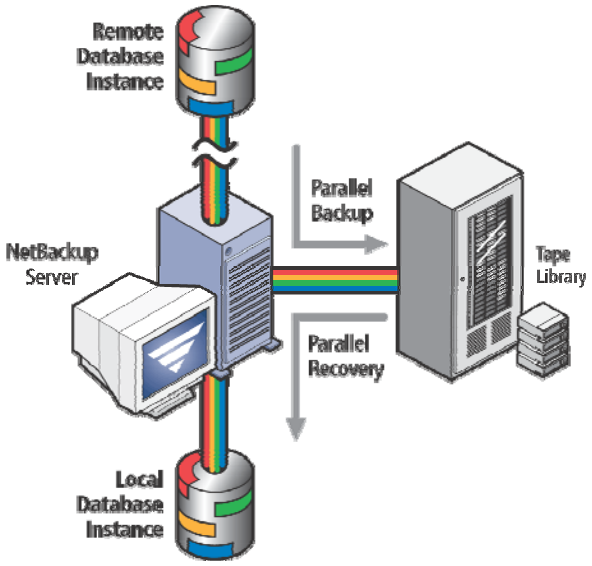


Figure 17: Online, high performance database backups enabled through multiplexing

NetBackup software also minimizes downtime by providing very fast recovery of databases, whole disks, or even entire sites in the event of a disaster. NetBackup software maximizes restore performance by recovering multiple data streams in parallel from a multiplexed tape or across multiple tape drives, especially when used with fast tape technologies provided by companies such as StorageTek, IBM, Quantum and all other leading tape drives and libraries. On systems with a locally attached tape device, NetBackup software optimizes throughput by utilizing shared memory and other high performance data transfer techniques. Whatever the environment, NetBackup software has the flexibility to provide continuous availability of databases or application-specific data with only minimal impact on user response times.

ORACLE
PartnerNetwork
CERTIFIED PARTNER

IBM
Business
Partner

Oracle and DB2 Database Protection

The NetBackup Advanced Client and Block Level Incremental Backup and Recovery

Oracle and DB2 backup and restore performance can be drastically increased by implementing the Block Level Incremental backup method that is available with the NetBackup Advanced Client. Online Oracle and DB2 database block level incremental (BLI) backups back up only changed file system blocks, virtually eliminating the backup window and significantly reducing the volume of data to be backed up and restored. The BLI method allows more frequent backups and continuous data availability while providing dramatically improved backup performance and significantly reducing CPU and network overhead on the Oracle/DB2 database server during backups. This functionality brings compelling benefits to large database environments because backups — both in data volume and time — now are only proportional to the amount of changed data, not sheer database size.

The BLI backups leverage VERITAS File System technology called storage checkpoint. The VERITAS Storage Foundation *for Databases* software product provides the storage checkpoint technology. Storage checkpoints identify and maintain a list of changed file system blocks as the data changes. No pre-processing is needed to find changed data blocks. Through a VERITAS File System API, NetBackup extracts only changed data blocks and can take either differential or cumulative block level incremental backups.

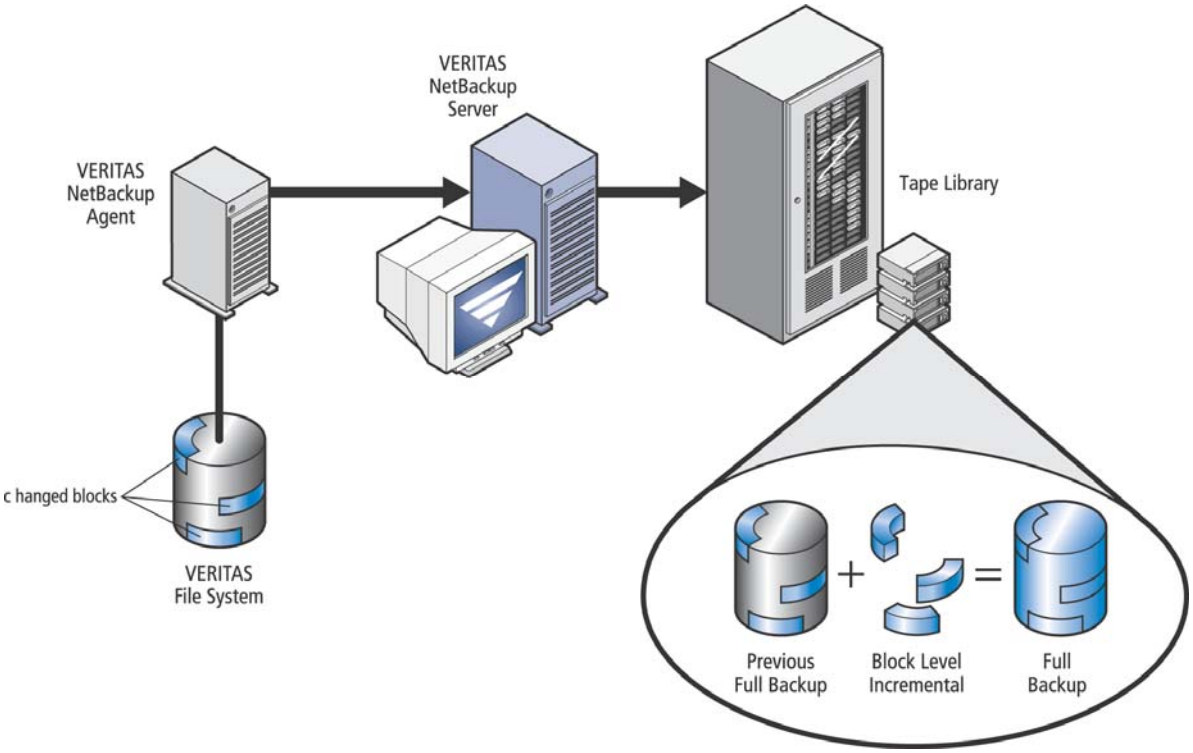


Figure 18: Online block level incremental backups

Automatic RMAN and DB2 Script Generation
Creating RMAN and DB2 scripts to perform Oracle or DB2 backup and recovery can be a tedious process, vulnerable to human error and requiring a certain level of technical sophistication to be done properly. NetBackup software has virtually eliminated this process by providing a graphical user interface that takes users through the process of configuring Oracle or DB2 backups. This graphical script generator allows administrators who are unfamiliar with script creation to quickly set up Oracle or DB2 backups or restores in a fraction of the time without having to know the scripting language or debug a script. This capability is currently available for Windows, Sun Solaris, HP-UX, IBM AIX, Red Hat and SUSE Linux environments. Additional Oracle support is available on HP Tru64 UNIX and SGI IRIX.

Archiving Data (Oracle Databases ONLY)
The ability to preserve database data for long periods of time and then retrieve it quickly is more crucial today than ever. The NetBackup for Oracle agent supports database-release-independent archiving. An entire database or a subset of database data may be extracted and archived. As a result, the user can quickly and efficiently import and restore this data into another database, without depending on the environment's original configuration, database version, machine operating system version or associated applications.

The NetBackup for Oracle agent accomplishes this feat through the use of the eXtensible Markup Language, also known as XML. For a backup, it exports selected database data by first converting the data into XML and then processing these XML files to tape or disk. The data can be maintained in this state indefinitely until a restore is required. The key value is that the data can be easily retrieved later, when the original set of databases, operating systems, and applications may not be available. With a restore request, the archived data is restored in XML format and is optionally inserted back into the database table of the user's choice. Since the NetBackup for Oracle agent works with an industry standard — XML — users can be confident that their business-critical database data will be available now and in the future. This capability is currently available for Oracle8i or later databases.

For additional information on Oracle backup and recovery methods, please reference the NetBackup for Oracle Backup and Recovery Essentials white paper.

Microsoft GOLD CERTIFIED Partner

Microsoft SQL Server Online Database Protection
VERITAS NetBackup software supports high-speed online backups of Microsoft SQL Server databases and all associated log files. Database administrators can quickly restore the complete SQL server database or individual files and file groups to any point in time with the easy-to-use administration GUI.

Key functionality includes:

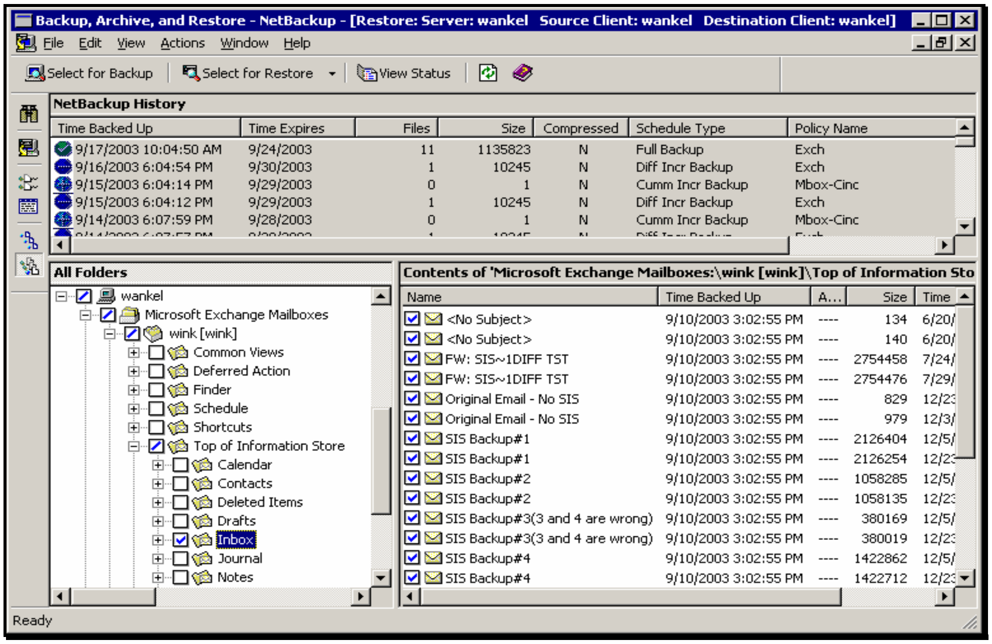
- **Flexible Data Protection Options** – Backup and recovery of databases, differentials, files, filegroups, and transaction logs. Read-only data backed up less frequently.
- **Superior Recovery** – Faster recovery as only damaged pages are recovered. Verify only restores can be used to verify SQL contents of a backup image without actually restoring the data.
- **Point-in-Time Recovery** – Recovers SQL databases to the exact point in time or transaction log mark by rolling forward only the transactions that occurred prior to a user-specified date and time.
- **Copy-Only Backups** – Create an on the fly full backup copy without interfering with an established backup sequence.
- **Granular Database View** – Display of database object properties delivers backup and recovery flexibility.

Microsoft Exchange Server Backup and Recovery
VERITAS NetBackup software utilizes Microsoft Exchange APIs to do online backups and recoveries of the Microsoft Exchange Information Store and Directory along with virtually all associated transaction log files.

VERITAS NetBackup for Exchange uses the Exchange Messaging API (MAPI) to enable "brick level" backups of Exchange mailboxes, allowing individual mailboxes, private and public folders or e-mail messages to be easily recovered. Administrators no longer need to rely on a spare server to restore individual messages from Exchange. Incremental Exchange mailbox backup and recovery is also supported.

VERITAS NetBackup for Exchange utilizes sophisticated Single Instance Storage technology to eliminate the redundancy inherent in mailbox-level backups, resulting in shorter backup times. VERITAS NetBackup for Exchange also provides options to limit backups to new email only, excluding deleted items, sent items or items already backed up during a previous backup session.

NEW with NetBackup 6.0: Off-Host backup for Microsoft Exchange 2003. The NetBackup Advanced Client is required to activate this functionality.



Backup, Archive, and Restore - NetBackup - [Restore: Server: wankel Source Client: wankel Destination Client: wankel]
File Edit View Actions Window Help
Select for Backup
Select for Restore
View Status
Ready

NetBackup History

Time Backed Up	Time Expires	Files	Size	Compressed	Schedule Type	Policy Name
9/17/2003 10:04:50 AM	9/24/2003	11	1135823	N	Full Backup	Exch
9/16/2003 6:04:54 PM	9/30/2003	1	10245	N	Diff Incr Backup	Exch
9/15/2003 6:04:14 PM	9/29/2003	0	1	N	Cumm Incr Backup	Mbox-Cinc
9/15/2003 6:04:12 PM	9/29/2003	1	10245	N	Diff Incr Backup	Exch
9/14/2003 6:07:59 PM	9/28/2003	0	1	N	Cumm Incr Backup	Mbox-Cinc

All Folders

- ☑ wankel
  - ☑ Microsoft Exchange Mailboxes
    - ☑ wink [wink]
      - ☐ Common Views
      - ☐ Deferred Action
      - ☐ Finder
      - ☐ Schedule
      - ☐ Shortcuts
      - ☑ Top of Information Store
        - ☐ Calendar
        - ☐ Contacts
        - ☐ Deleted Items
        - ☐ Drafts
        - ☑ Inbox
        - ☐ Journal
        - ☐ Notes

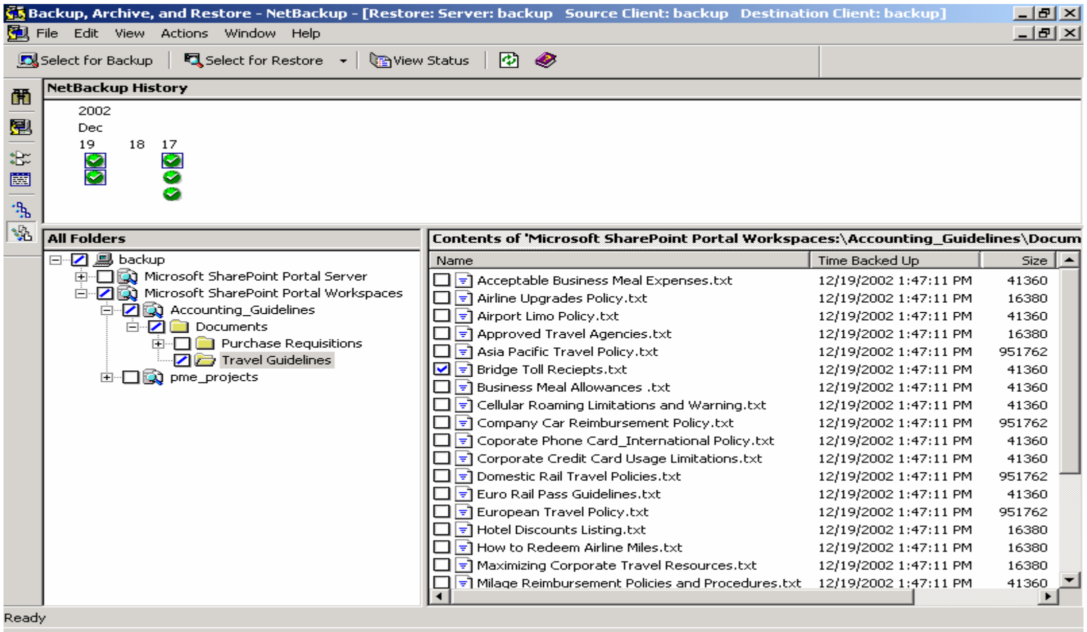
Contents of 'Microsoft Exchange Mailboxes:\wink [wink]\Top of Information Sto

Name	Time Backed Up	A...	Size	Time
☑ <No Subject>	9/10/2003 3:02:55 PM	----	134	6/20/
☑ <No Subject>	9/10/2003 3:02:55 PM	----	140	6/20/
☑ FW: SIS~1DIFF TST	9/10/2003 3:02:55 PM	----	2754458	7/24/
☑ FW: SIS~1DIFF TST	9/10/2003 3:02:55 PM	----	2754476	7/29/
☑ Original Email - No SIS	9/10/2003 3:02:55 PM	----	829	12/2
☑ Original Email - No SIS	9/10/2003 3:02:55 PM	----	979	12/3/
☑ SIS Backup#1	9/10/2003 3:02:55 PM	----	2126404	12/5/
☑ SIS Backup#1	9/10/2003 3:02:55 PM	----	2126254	12/2
☑ SIS Backup#2	9/10/2003 3:02:55 PM	----	1058285	12/5/
☑ SIS Backup#2	9/10/2003 3:02:55 PM	----	1058135	12/2
☑ SIS Backup#3(3 and 4 are wrong)	9/10/2003 3:02:55 PM	----	380169	12/5/
☑ SIS Backup#3(3 and 4 are wrong)	9/10/2003 3:02:55 PM	----	380019	12/2
☑ SIS Backup#4	9/10/2003 3:02:55 PM	----	1422862	12/5/
☑ SIS Backup#4	9/10/2003 3:02:55 PM	----	1422712	12/2

Figure 19: VERITAS NetBackup provides a broad glimpse into Exchange's backup history, allowing administrators to easily perform database, mailbox, or message recovery

Microsoft SharePoint Portal Server Backup and Recovery

NetBackup software integrates with the Microsoft SharePoint Portal (SPS) APIs, delivering comprehensive data protection for SPS and offers protection of all components of the SharePoint Portal server, including web store data, MS Search Service system resources and SPS configuration information. The easy to use point-and-click GUI simplifies the selection of SPS components for backup and recovery.


Backup, Archive, and Restore - NetBackup - [Restore: Server: backup Source Client: backup Destination Client: backup]
File Edit View Actions Window Help
Select for Backup
Select for Restore
View Status

NetBackup History

2002
Dec
19 18 17

All Folders

- ☑ backup
  - □ Microsoft SharePoint Portal Server
  - ☑ Microsoft SharePoint Portal Workspaces
    - ☑ Accounting_Guidelines
      - ☑ Documents
        - □ Purchase Requisitions
        - ☑ Travel Guidelines
    - □ pme_projects

Contents of 'Microsoft SharePoint Portal Workspaces:\Accounting_Guidelines\Docum

Name	Time Backed Up	Size
□ Acceptable Business Meal Expenses.txt	12/19/2002 1:47:11 PM	41360
□ Airline Upgrades Policy.txt	12/19/2002 1:47:11 PM	16380
□ Airport Limo Policy.txt	12/19/2002 1:47:11 PM	41360
□ Approved Travel Agencies.txt	12/19/2002 1:47:11 PM	16380
□ Asia Pacific Travel Policy.txt	12/19/2002 1:47:11 PM	951762
☑ Bridge Toll Reciepts.txt	12/19/2002 1:47:11 PM	41360
□ Business Meal Allowances .txt	12/19/2002 1:47:11 PM	41360
□ Cellular Roaming Limitations and Warning.txt	12/19/2002 1:47:11 PM	41360
□ Company Car Reimbursement Policy.txt	12/19/2002 1:47:11 PM	951762
□ Coporate Phone Card_International Policy.txt	12/19/2002 1:47:11 PM	41360
□ Corporate Credit Card Usage Limitations.txt	12/19/2002 1:47:11 PM	41360
□ Domestic Rail Travel Policies.txt	12/19/2002 1:47:11 PM	951762
□ Euro Rail Pass Guidelines.txt	12/19/2002 1:47:11 PM	41360
□ European Travel Policy.txt	12/19/2002 1:47:11 PM	951762
□ Hotel Discounts Listing.txt	12/19/2002 1:47:11 PM	16380
□ How to Redeem Airline Miles.txt	12/19/2002 1:47:11 PM	16380
□ Maximizing Corporate Travel Resources.txt	12/19/2002 1:47:11 PM	16380
□ Milage Reimbursement Policies and Procedures.txt	12/19/2002 1:47:11 PM	41360

Ready

Figure 20: Share Point Portal Agent

SOFTWARE
SAP
GLOBAL PARTNER

Online SAP NetWeaver Backup and Recovery

With large-scale SAP NetWeaver environments requiring 24x7 operations, data protection becomes an essential component of any successful SAP NetWeaver deployment plan. The integration of VERITAS NetBackup software and online SAP data backup utilities provides a comprehensive approach to SAP NetWeaver data protection. VERITAS NetBackup for SAP NetWeaver provides high performance, online backup of SAP NetWeaver environments, optimal utilization of large scale device and robotic configurations, and a scalable, distributed design.

What's New with NetBackup 6.0

New functionality that is available with NetBackup 6.0 for SAP is as follows:

- NetBackup for SAP integration with Oracle RMAN
- SAP BACKINT support for MaxDB (SAP DB)

Figure 21 below diagrams a SAP NetWeaver backup configuration. SAP NetWeaver backups can be scheduled and automatically initiated via the NetBackup scheduler or via the SAPDBA interface. NetBackup software supports the SAP NetWeaver BACKINT interface specification for backup, restore and inquire functions from the respective SAP NetWeaver tools (brbackup, brrestore, and brarchive). BACKINT then starts the required NetBackup programs, monitors the progress of each program, and reports the results back to the SAP NetWeaver tool upon completion. NetBackup for SAP software supports SAP NetWeaver Oracle database backups as either raw partitions or regular files. NetBackup for SAP also support MaxDB (SAP DB) backup and recovery.

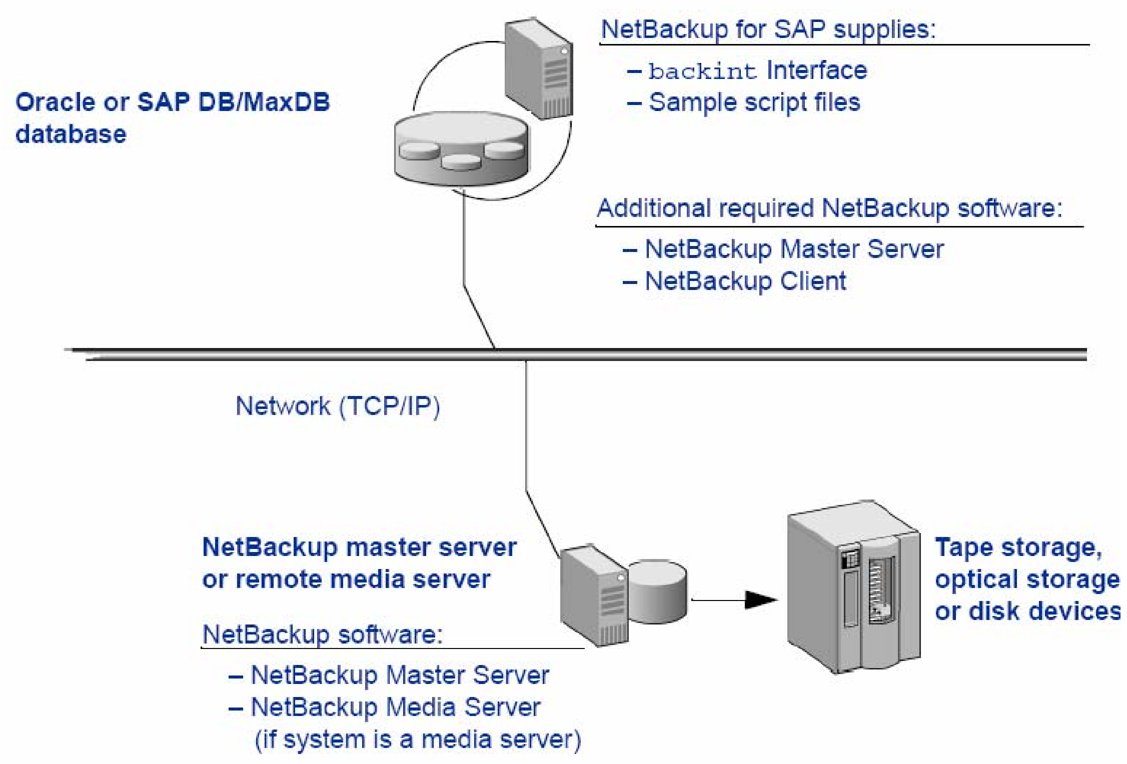

Oracle or SAP DB/MaxDB database
NetBackup for SAP supplies:
– backint Interface
– Sample script files
Additional required NetBackup software:
– NetBackup Master Server
– NetBackup Client
Network (TCP/IP)
NetBackup master server or remote media server
NetBackup software:
– NetBackup Master Server
– NetBackup Media Server (if system is a media server)
Tape storage, optical storage or disk devices

Figure 21: NetBackup support for SAP NetWeaver environments

For additional information on NetBackup for SAP data protection, please reference the NetBackup for SAP Environment Protection white paper.

RUNS WITH LOTUS .domino.

High Performance Lotus Backup and Recovery

NetBackup software supports online backup of Lotus Notes and Domino Server version R4, R5, R6 and R7. NetBackup for Lotus Notes also supports backing up R5, R6 and R7 transaction logs, so that the database may be recovered to a specific point-in-time. However, Domino Server manages the actual recycling of transaction logs.   The type of Domino Server backup that is run will determine whether or not the logs are marked for recycling. The following types of backups are supported with NetBackup for Lotus Notes:

- **Full Backup** — Backs up all Lotus databases, logged or unlogged, specified in the file list and/or transaction logs, if the BACKUP_TRANSACTION_LOGS directive is found in the file list.
- **Differential Incremental Backup** — When NetBackup software performs a differential incremental backup on unlogged or local databases, it will only backup those unlogged or local databases specified in the file list that have been modified since the last full or differential incremental backup. The last modification date is determined by the time the database was last modified, not the time/date stamp of the database file. For logged databases, the NetBackup software will only backup those logged databases identified in the file list that have been assigned a new DBIID since the last full or differential incremental backup.
- **Cumulative Incremental Backup** — When NetBackup software performs a cumulative incremental backup on unlogged or local databases, it will only backup those unlogged or local databases specified in the file list that have been modified since the last full backup. Once again, the last modification date is determined by the time the database was last modified, not the time/date stamp of the database file. For logged databases, NetBackup software will backup only those logged databases identified in the file list that have been assigned a new DBIID since the last full backup.
- **User Backup** — Actions performed for a user backup are identical to a full backup except that the transaction logs are not marked as ready to be recycled after they are successfully backed up. Because transaction logs are not recycled, user backups are like taking a snapshot of the databases at a given point in time without impacting the content of ongoing full and incremental backups.

NDMP BACKUPS OF NETWORK-ATTACHED STORAGE (NAS)

VERITAS NetBackup™ software provides online data backup and restore for Network-Attached Storage (NAS) hosts using the Network Data Management Protocol (NDMP). In a NetBackup NDMP configuration, only control and catalog information is transferred over the network. This is a critical requirement in NAS host environments where file servers can store a terabyte or more of online data, which makes network-based backups infeasible or even impossible.

In a typical NetBackup NDMP configuration (see Figure 22 below), a NetBackup server sends backup, recovery and robotic control commands via the NDMP protocol to the NAS file server. The NetBackup catalog maintains a complete listing of the backup image. The NAS NDMP host performs the actual NDMP backup/restore utility that runs on the NAS file server and carries out the NDMP commands from NetBackup. Large tape libraries can be shared between NAS file servers or between NetBackup master/media servers and NAS file servers.

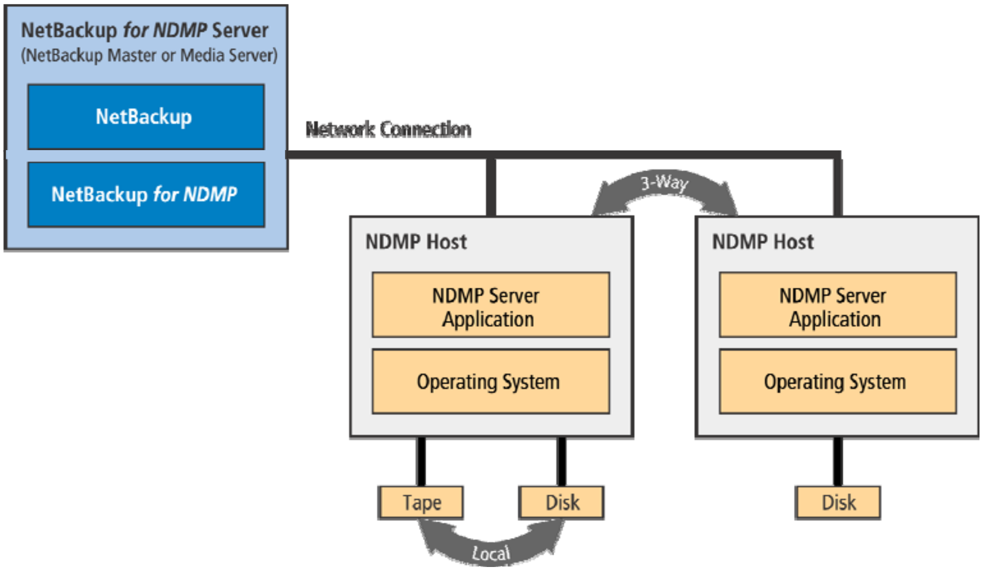


Figure 22: NetBackup tape backups of NAS servers via NDMP

SUPPORTED NDMP CONFIGURATIONS

The following sections describe specific supported NDMP configurations and capabilities, providing unparalleled flexibility in defining and implementing a NAS backup strategy.

NDMP Backups

NetBackup software supports backing up NAS server (using NDMP software) to locally attached tape storage devices. However, there are times when it is not cost effective to directly attach a tape drive or library to each NDMP host, especially in environments where there are many smaller NAS servers. For this reason, NetBackup software offers tremendous flexibility for alternate NAS server backup techniques (see Figure 22 below). NetBackup software supports backing up from one NAS server over the network to another NAS server with locally attached storage devices and restoring from a NAS server with locally attached storage devices over the network to another NAS server. This capability is known as “3-way backup/restore.” In situations where there are no storage devices attached to any NAS server within an enterprise, NetBackup software supports backing up the NAS server to a NetBackup server and restoring the NAS data from a NetBackup server to the NAS server. Also known as “Remote NDMP,” this functionality leverages NDMP and does not utilize any NFS/CIFS mounting.

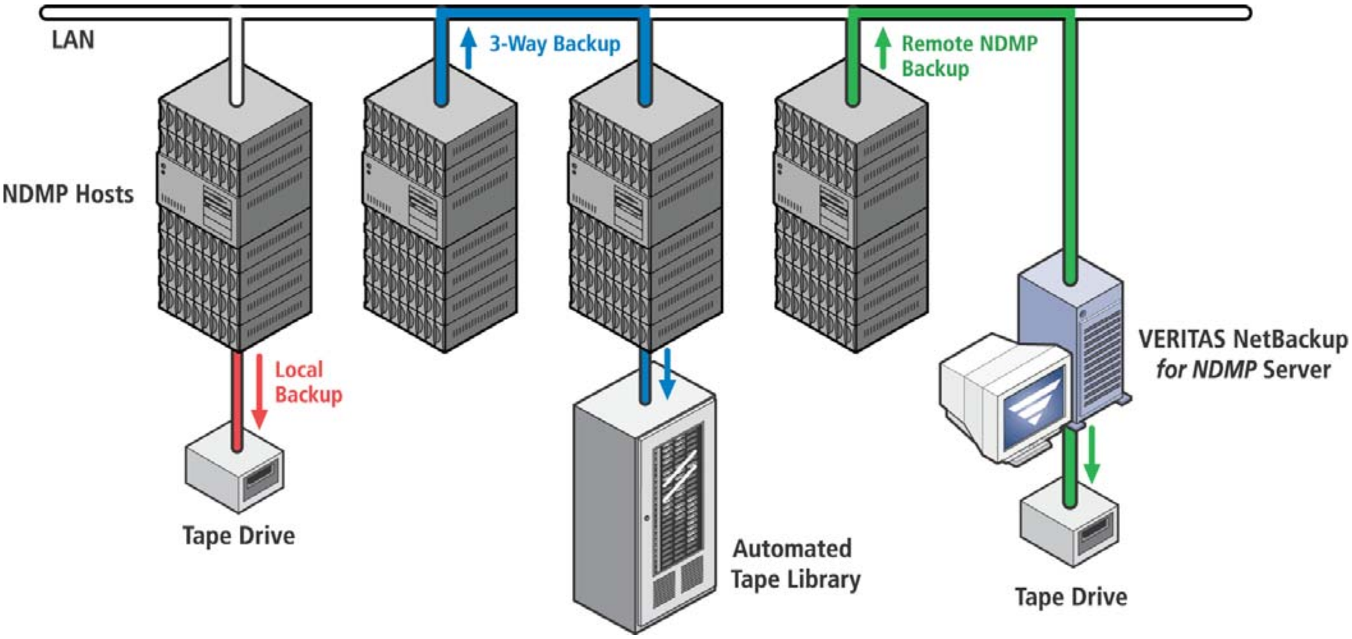


Figure 23: NDMP–to-NDMP backups

Direct Access Recovery (DAR)

NetBackup for NDMP can use Direct Access Recovery during NDMP restores. DAR greatly reduces the time it takes to restore files since a single file can be restored without having to read the entire image. DAR can be used when restoring files, but not when restoring directories. NetBackup software automatically determines whether using Direct Access Recovery will result in a faster restore and utilizes DAR if it will be beneficial. The NDMP host must support DAR to perform recoveries.

Library sharing between NetBackup and NDMP Hosts

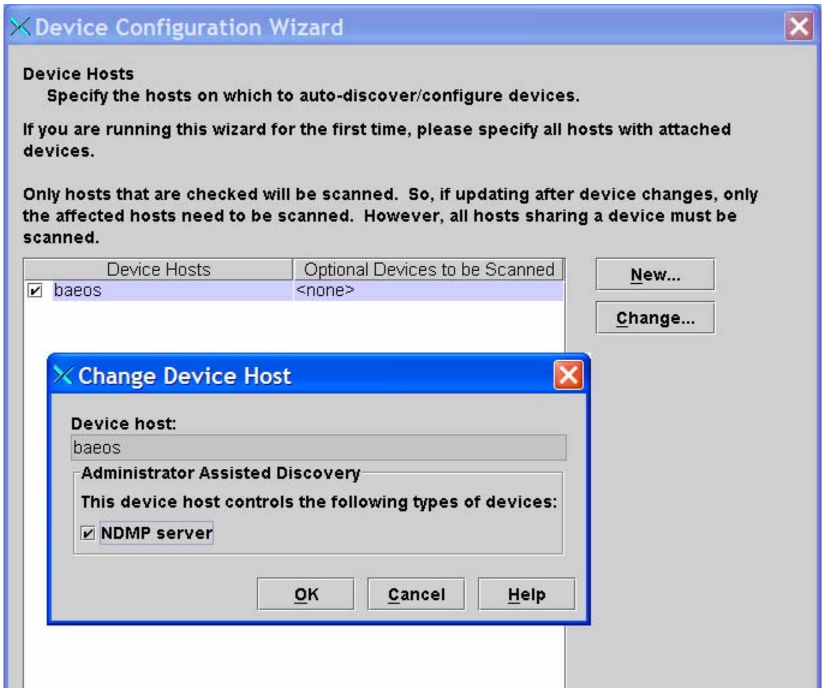
NetBackup for NDMP can share a tape library between the NetBackup server and one or more NDMP NAS servers, or just between the NDMP NAS servers themselves. For more information, see the “Sharing Tape Libraries” section later in this white paper.

Shared Storage Option (SSO) for NDMP

NetBackup allows for the sharing of tape drives among NetBackup media servers and NDMP devices. This includes support for library types LTD, TL8, ACS and TLH. All drive types within supported libraries as well as standalone drives are supported.

Auto-Discovery for NDMP Attached Devices

NetBackup media manager provides complete management and control of the devices and media used for backups and restores of NDMP hosts. The NetBackup Device Configuration wizard can auto-discover and configure storage devices that are attached to an NDMP host. This significantly reduces the NDMP configuration complexity. An example of the NetBackup Device Configuration wizard is shown in Figure 24 below:



Device Configuration Wizard

Device Hosts
Specify the hosts on which to auto-discover/configure devices.

If you are running this wizard for the first time, please specify all hosts with attached devices.

Only hosts that are checked will be scanned. So, if updating after device changes, only the affected hosts need to be scanned. However, all hosts sharing a device must be scanned.

Device Hosts	Optional Devices to be Scanned
☑ baeos	<none>

Change Device Host

Device host: baeos

Administrator Assisted Discovery

This device host controls the following types of devices:

☑ NDMP server

Figure 24: NetBackup Device Configuration wizard

VERITAS NETBACKUP BACKUP AND RECOVERY CONCEPTS

The following sections explain the basic concepts involved in backup operations.

STORAGE UNITS

VERITAS NetBackup software associates all storage devices and media with logical storage units. As used by NetBackup, the term storage unit refers to a logical entity that includes one or more physical storage devices that are of a specific type and media density and attached to a specific host. There are three categories of storage units:

- Directly attached standalone or robotic media storage units that contain tape or optical devices and are managed by the VERITAS NetBackup Enterprise Media Manager (EMM).
- Standalone or robotic storage units controlled by the VERITAS NetBackup media manager via Network Data Management Protocol (NDMP).
- Disk file system storage units consisting of a designated directory in the file system that will receive the backup or archive data.

During configuration, the NetBackup administrator first completes any necessary device and media configuration and then groups all devices and media into appropriate VERITAS NetBackup storage units. For example, for a specific host a Hewlett-Packard optical disk library could be in one storage unit and an ATL tape library could be in another. Priorities may be assigned to individual storage units and/or to individual devices within a storage unit. This provides extreme flexibility with the preference of storage unit selection, should the administrator choose to have VERITAS NetBackup™ software determine which storage unit to use during a backup. During backups and restores, VERITAS NetBackup specifies the media required and VERITAS NetBackup EMM automatically finds it and mounts it in a device within an available storage unit.

The storage unit concept makes it easier to configure backups because the administrator can simply assign the storage unit with the type of storage needed for a client backup, rather than worry about specific devices. It also provides a virtual approach to backup storage because if more storage of that type is needed, it will be automatically and transparently utilized after being added to the VERITAS NetBackup EMM and VERITAS NetBackup configurations.

VERITAS NETBACKUP POLICIES

An important feature of VERITAS NetBackup software is the capability to configure backup policies. A policy consists of one or more clients that have similar backup needs. Every VERITAS NetBackup client must belong to at least one policy and often belongs to more than one. Policies were formerly known as classes in earlier versions of NetBackup software.

The major advantage offered by VERITAS NetBackup policies is that the administrator can group clients into policies and then configure backups for the entire group, rather than one client at a time. In addition, since a client can belong to more than one policy, the administrator can establish different schedules for different files on the same client or assign a client to one policy for automatic backups and another for user-directed backups and archives.

When new clients are installed, they can be added to an existing policy or the administrator can define new policies for new clients on a one-by-one basis. An easy way to create a new policy is simply to clone and modify an existing one.

The properties that the administrator configures for each policy include:

- **Files** — Lists the set of files to include in automatic backup operations for the policy. It is not a requirement that all files on the list exist on all clients and it is often convenient to make the file list a superset of the desired files.

The administrator or user can also specify a list of files to exclude from each client backup. The exclude list is not part of the policy definition and is unique for each client.

- **Clients** — Lists the set of clients in the policy. When a new client is added to VERITAS NetBackup, the administrator can simply add the client's host name to the appropriate policy and the client software can optionally be installed automatically over the network.
- **Schedules** — Lists the set of schedules pertaining to the policy.
- **Policy Type** — Specifies the type of policy you are configuring. You will use the Standard policy type for most UNIX clients. For Windows clients, you will use the MS-Windows-NT policy type. The other policy types cover special cases. For example, you would specify the Microsoft Exchange Server backup type to backup Microsoft Exchange clients or the Oracle backup type to back up Oracle databases on clients that are running Oracle.
- **Policy Storage Unit** — Specifies the type of storage device to receive the file backups. This is an optional feature. If unspecified, backups and archives can go to any available storage unit. Priorities may be set so that the backups and archives may be directed first to available storage units with higher priority.
- **Policy Volume Pool** — Specifies the set of volumes (i.e. media) to use for storing the backups. If unspecified, backups and archives use the default NetBackup volume pool.
- **Policy Attributes** — The following are policy-specific attributes:
    - **Limit Jobs Per Policy** — Specifies the number of client jobs from this policy that can be performed concurrently. Administrators can use this parameter to "balance" network load.
    - **Job priority** — Specifies the priority of backups for a policy relative to the other policies. This is useful to ensure that the most important data is backed up first.
    - **Keyword Phrase** — Enables a policy to be defined by a unique name, which the administrator may browse for during a restore. The default setting lists no keyword phrase.
    - **Active** — Specifies whether or not NetBackup will allow backups or archives for this policy. This is useful for temporarily deactivating a policy during, for example, network troubleshooting or repair. The administrator may also specify the date and time the policy becomes active.
    - **Backup Network Drives** — Specifies whether to allow backups of remote files that are NFS mounted on the client.
    - **Cross Mount Points** — Specifies whether or not VERITAS NetBackup software is to cross file systems to back up directory paths and files.
    - **Collect True Image Restore Information** — Specifies whether NetBackup software will collect the information necessary to support true image recovery of directories saved by clients in this policy. For more information, see the section on True Image Restore below.
    - **Image Compression** —Specifies whether or not to use software image compression during backup operations.
    - **Encryption** — Specifies whether or not to enable client-level encryption during backup operations. Several levels of encryption are supported. Encryption is a separately priced NetBackup option.

All policy definitions are stored in the configuration database on the NetBackup master server. In networks with more than one storage domain of VERITAS NetBackup servers, clients can belong to policies on more than one master server. Although clients will normally use only one master server, the ability to use others can be an essential feature if a client's regular master server goes down and there is critical data to back up.

SCHEDULING

Each VERITAS NetBackup policy has a set of schedules to control its backups and archives. These schedules are part of the policy definition and each schedule for a policy affects the entire list of clients and files in that policy.

A typical policy might call for a weekly full backup followed by incremental backups every other day, as illustrated in Figure 25 below:

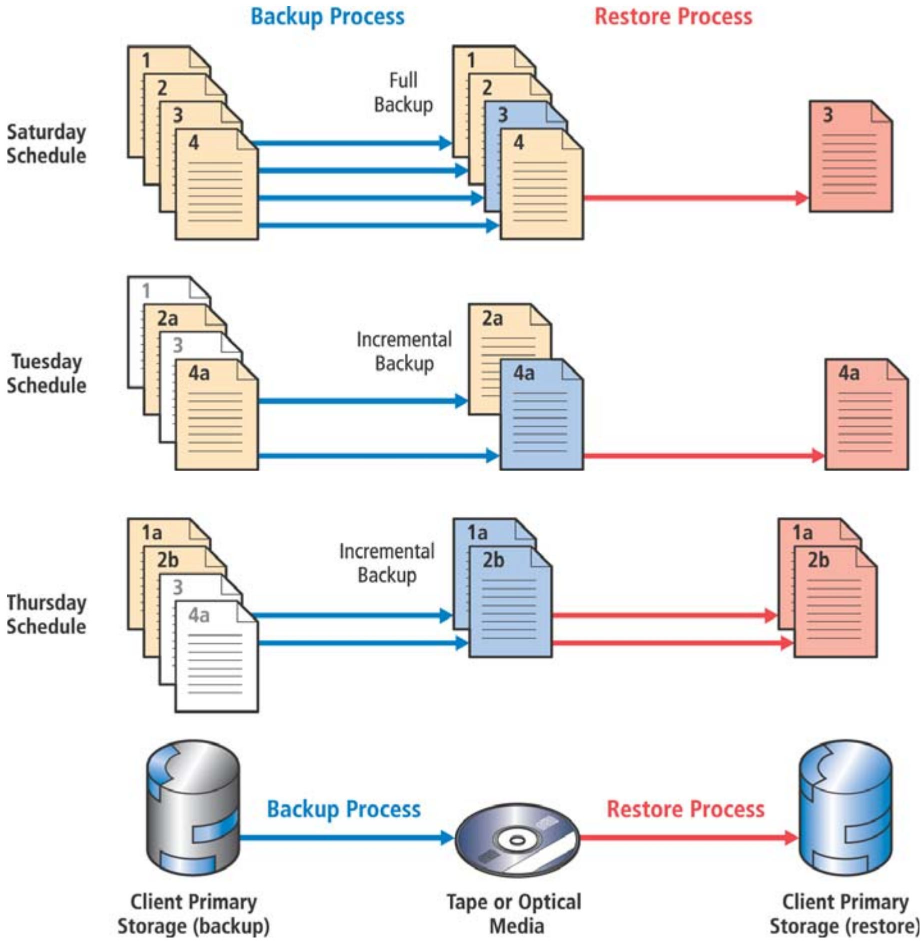


Figure 25: Full and incremental backup scheduling

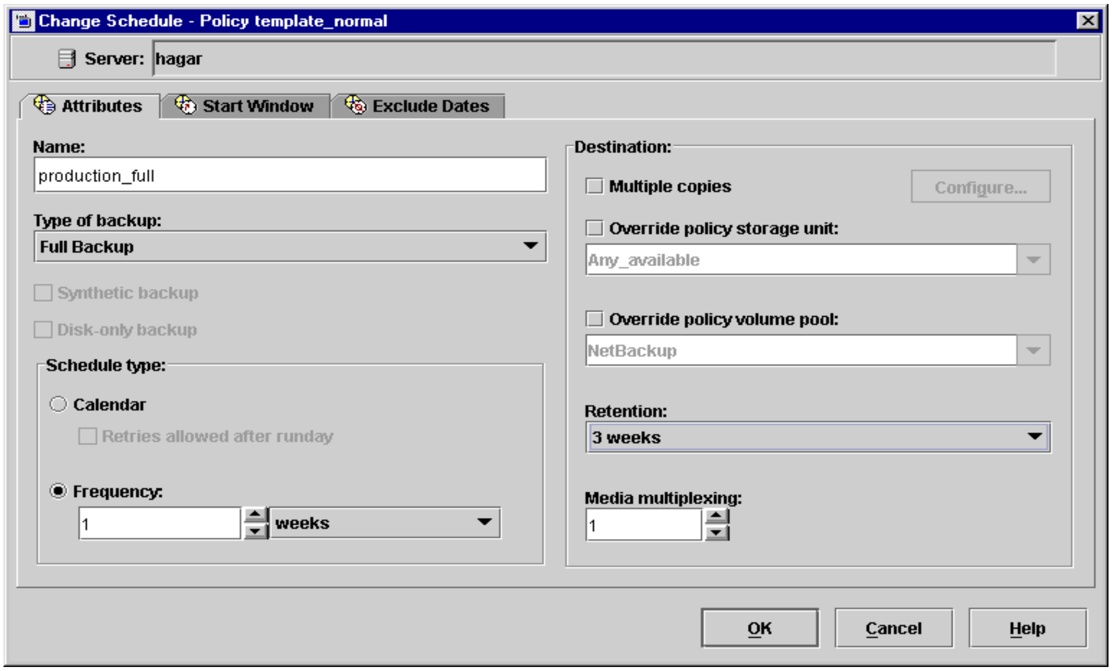
Among the attributes that the administrator specifies for each schedule are:

- **Type of Backup** — There are 5 basic backup types: full, cumulative incremental, differential incremental, user backup and user archive.
- **Backup Window** – Specifies the backup window, which is the time period during which backups can occur for this schedule. The start time defines the times and days of the week when the window is open. The duration defines how long the backup window stays open. For example, the administrator could schedule automatic full backups to occur during early morning hours on weekends, when the increase in network traffic will have the least effect on users.
- **Schedule Type** — VERITAS NetBackup software may automate backup policies using calendar-based scheduling methods, frequency-based scheduling methods, or a combination of both techniques.
- **Calendar** — Enables the administrator to configure backups that initiate on specific days (see Figure 25 below). Schedules may be designed to reoccur daily, weekly, or monthly. Furthermore, specific days may be excluded

from a schedule. For example, a user may create a backup schedule that does not commence on the last day of each calendar quarter.

- **Frequency** — Specifies the period of time that will elapse until the next backup operation can begin with a predefined schedule. For example, if the frequency is seven days and a successful full backup occurs on Wednesday, the next full backup does not occur until the following Wednesday. The frequency can be set to a value that preserves all critical changes in the files. If data changes often, the frequency can be short. For more stable files, the frequency can be longer. Incremental backups will have a shorter frequency than full backups.
- **Multiple Copies** — The Inline Copy feature allows the NetBackup user to create up to four duplicates of the backup job concurrently with the primary backup. Each duplicate copy may be assigned a unique retention period. Given adequate disk or tape device resources, Inline Copy makes duplication much more efficient by combining the tasks of backup and duplication into one activity. Multiple copies can be made to either disk or tape.
- **Override Policy Storage Unit** — Specifies the storage device to receive the file backups. This option overrides the storage unit specified at the policy level and provides the flexibility for putting backups from different schedules on different storage units. For example, it may be desirable to put full backups and incremental backups on different types of media.
- **Override Policy Volume Pool** — Specifies the set of volumes (e.g. media) to use for storing the file backups. This option overrides the pool specified at the policy level and allows the administrator to keep images from different schedules on separate sets of volumes.
- **Retention** — Indicates a specific time period for keeping backup or archive copies of files before deleting them from secondary storage. While retention periods may range from one week (Level 0) to infinite (Level 24), the default is two weeks (Level 1), and the NetBackup administrator may set the retention period to a specific level. The retention level also denotes a schedule’s priority within the policy, with Level 24 schedules having the highest priority and Level 0 the lowest.
- **Media Multiplexing** — Specifies the number of jobs from a particular schedule that NetBackup can multiplex onto any one drive.

The above attributes give the administrator great latitude. Schedules can range from very basic to schemes that are sophisticated enough to meet the most demanding backup requirements. Examples of NetBackup software’s scheduling functionality is shown in Figures 26 and 27 below:



Change Schedule - Policy template_normal

Server: hagar

Name: production_full

Type of backup: Full Backup

□ Synthetic backup

□ Disk-only backup

Schedule type:

○ Calendar

□ Retries allowed after runday

● Frequency: 1 weeks

Destination:

□ Multiple copies

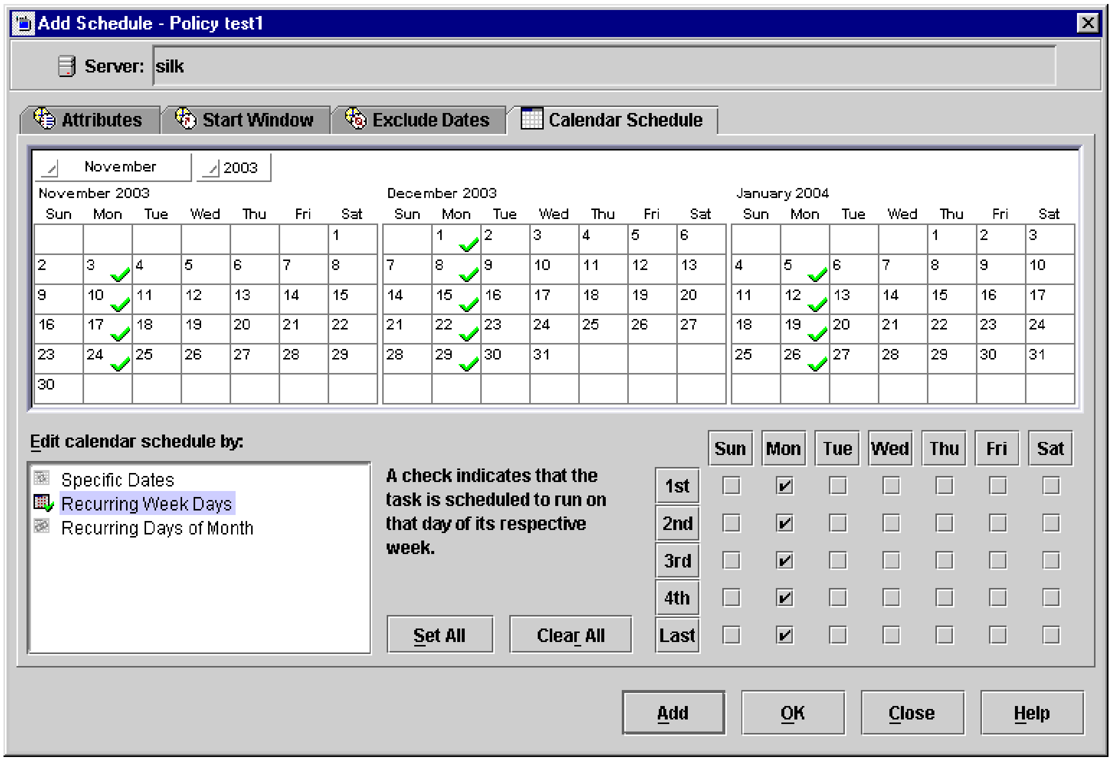
□ Override policy storage unit: Any_available

□ Override policy volume pool: NetBackup

Retention: 3 weeks

Media multiplexing: 1

Figure 26: Backup schedule administration GUI



Add Schedule - Policy test1

Server: silk

November 2003

Sun	Mon	Tue	Wed	Thu	Fri	Sat
						1
2	3 ✓	4	5	6	7	8
9	10 ✓	11	12	13	14	15
16	17 ✓	18	19	20	21	22
23	24 ✓	25	26	27	28	29
30						

December 2003

Sun	Mon	Tue	Wed	Thu	Fri	Sat
	1 ✓	2	3	4	5	6
7	8 ✓	9	10	11	12	13
14	15 ✓	16	17	18	19	20
21	22 ✓	23	24	25	26	27
28	29 ✓	30	31			

January 2004

Sun	Mon	Tue	Wed	Thu	Fri	Sat
				1	2	3
4	5 ✓	6	7	8	9	10
11	12 ✓	13	14	15	16	17
18	19 ✓	20	21	22	23	24
25	26 ✓	27	28	29	30	31

Edit calendar schedule by:

- Specific Dates
- Recurring Week Days
- Recurring Days of Month

A check indicates that the task is scheduled to run on that day of its respective week.

	Sun	Mon	Tue	Wed	Thu	Fri	Sat
1st	□	☑	□	□	□	□	□
2nd	□	☑	□	□	□	□	□
3rd	□	☑	□	□	□	□	□
4th	□	☑	□	□	□	□	□
Last	□	☑	□	□	□	□	□

Figure 27: Backups may be scheduled to initiate on specific days

NETBACKUP CATALOG PROTECTION

In order for NetBackup to restore any file, NetBackup needs information from the NetBackup catalog to determine where the backup for the file is located. Without a catalog, NetBackup cannot restore data.

Because the catalog plays an integral part in a NetBackup environment, the catalog must be protected by a particular type of backup--a catalog backup. A catalog backup backs up catalog-specific data as well as produces disaster recovery information.

New with NetBackup 6.0: Online (hot) NetBackup catalog protection.

The new NetBackup online (hot) catalog backup functionality has been designed to provide the following:

- Hot NetBackup catalog backup capability to support 24x7 backup environments
- Enable all the features which NetBackup standard backup provides for catalog backup
- Enable the catalog backup to take advantage of all of the features of the standard NetBackup policy type
- Improved NetBackup catalog recover procedures

NetBackup Catalog Backup Configuration

A catalog backup is configured separately from regular client backups by using the Catalog Backup Wizard. The catalog can be stored on a variety of media.

This type of catalog backup is for highly active NetBackup environments in which continual backup activity is typically occurring. It is considered an online, hot method because it can be performed while regular backup activity is taking place. This type of catalog is policy-based and can span more than one tape.

Online, hot catalog backups use media from the Catalog Backup volume pool only.

Online NetBackup catalog protection is policy-based, which means that it has all of the scheduling flexibility of a regular backup policy. This catalog backup type is designed for use in highly active NetBackup environments where there is usually backup activity taking place.

The online, hot catalog backup can do the following:

- Can back up the catalog while continual client backups are in progress.
- Can span multiple tapes for a catalog backup.
- Allows for a flexible pool of catalog tapes.
- Can perform a full or incremental catalog backup.
- Can restore the catalog to a different location.
- Can run scheduled catalog backups.
- Offers a wizard to automate the catalog recovery process or a guided command line tool.
- Appends to existing data on tape.
- Can be duplicated.

An online NetBackup catalog backup can be configured using one of the following methods:

- By using the Catalog Backup Wizard.
- By using the Backup Policy Configuration Wizard.
- By selecting the NetBackup Catalog type when creating a backup policy.

STRATEGIES TO ENSURE SUCCESSFUL NETBACKUP CATALOG BACKUPS

Below are some tips and tricks to successful NetBackup online catalog protection.

- Use only those methods described in the NetBackup System Administrator's Guide to back up the NetBackup catalogs. The methods described there are the only operations that can track all relevant NetBackup activities and ensure consistency between the catalog files.
- Back up the catalogs frequently and on a regular basis. If a catalog backup is lost, you lose information about backups and configuration changes that were made between the time of the last NetBackup catalog backup and the time that the disk crash occurred.
- Never manually compress the catalogs, or NetBackup may not be able them using bprecover.
- If you back up your catalogs to disk (not recommended), always back up to a different disk than where the catalogs reside. If you back up to the same disk and that disk fails, you will also lose the catalog backups in addition to the catalogs and recovery will be much more difficult. Also, ensure that the disk has enough space for the catalogs or it will fill up and backups will fail.
- The NetBackup binary image catalog is more sensitive to the location of the catalog. Storing the catalog on a remote file system may have critical performance issues for catalog backups. NetBackup does not support saving catalogs to a remote file system such as NFS or CIFS.

Considerations if running cold, offline catalog backups:

- If you are using media servers, be sure to manually alter the NetBackup catalog configuration to include the catalogs on the media servers.
- Keep a hard-copy record of the media IDs where you store the NetBackup catalog backups, or include the administrator's e-mail address in the Global Attributes properties. The e-mail that the administrator receives includes the status of each catalog backup and the media ID that was used. Print the e-mail or save it on a disk other than the disk containing the catalogs.
- If sending catalog backups to a robot or tape stacker, a second standalone tape drive, or to disk, choose either of the two automatic backups: **After each session of scheduled, usr, or manual backups** or **After each session of scheduled backups**
- If using a single, standalone tape drive to back up both catalog *and* regular business data, choose either:
  - **After each session of scheduled backups** if you will be running only one backup session per day or night, or
  - **Only when manually initiated** if you will be running multiple backup sessions in a single day or night

  Because NetBackup will not place catalog and regular backups on the same tape, both methods require you to swap tapes.

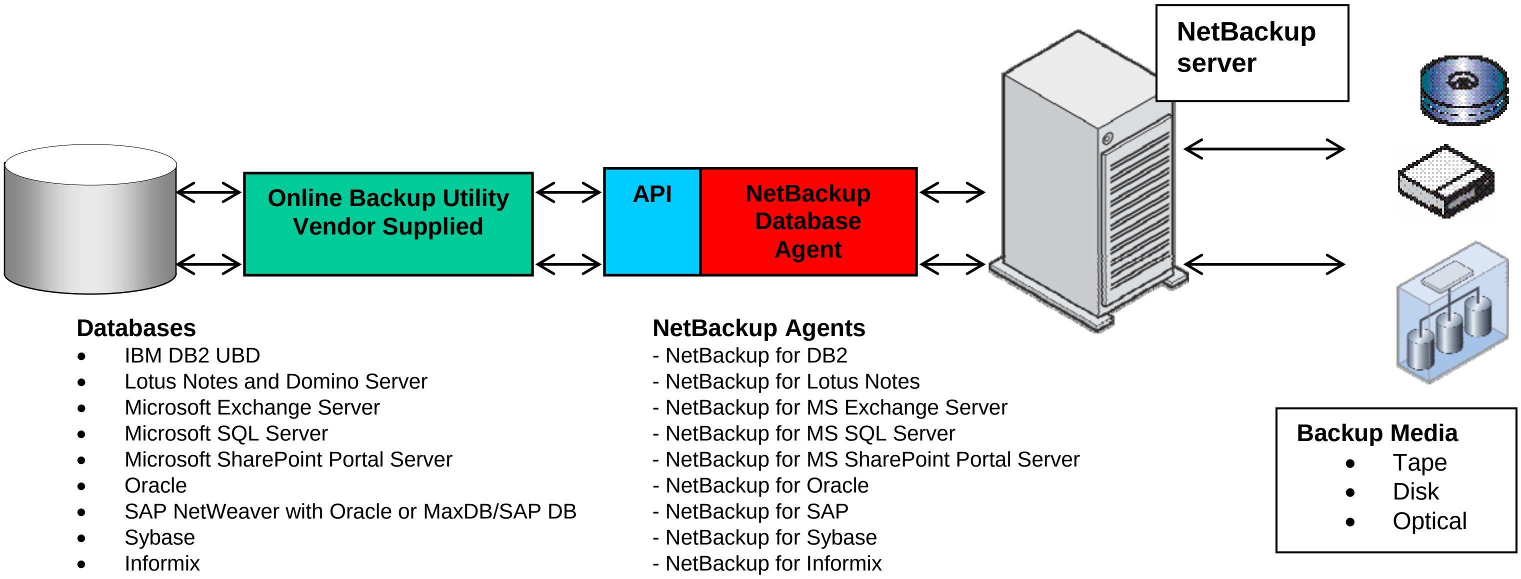
  The general procedure for catalog backups when you have only one standalone drive is as follows:

  a. Insert the tape configured for catalog backups.
  b. Manually start the backup.
  c. When the backup is complete, remove the tape and store it in a safe place.

DATABASE BACKUP METHODS

VERITAS NetBackup™ software supports three methods of backing up relational database management systems: raw (i.e. cold), warm and online (i.e. hot). Cold database backup involves shutting down the database and using the raw partition file system backup capability of NetBackup. Warm database backups use pre- and post-processing NetBackup scripts to place the database in "online backup" mode, then proceed to back up the database raw partition or database file. Online database backups for Oracle, Microsoft SQL Server, IBM DB2, Sybase and Informix use the VERITAS NetBackup database backup agents. These agents integrate with native database application programmer's interfaces (APIs) or backup utilities, such as Oracle Recovery Manager (RMAN) or Informix ON-Bar. Specifics of the database backup methods supported by NetBackup software are outlined below.

- **Raw database backups** (e.g. database files or partitions) are configured and executed in the same manner as file backups. The performance resulting from backing up cold databases is generally greater than that achieved when backing up through the UNIX file system or through the data extraction utilities supplied by RDBMS vendors.
- **Warm database backup** is similar to raw database or file backup method described above, except that the database is placed in "hot backup" mode via the capability of NetBackup software to pre-process scripts prior to the raw partition or database file backup. After the backup is completed, the database is returned to normal mode via a NetBackup post-processing script.
- **Hot database backup** requires a VERITAS NetBackup database backup agent and a corresponding database vendor backup utility. NetBackup database backup agents exist for Oracle, Microsoft SQL Server, Microsoft Exchange Server, Lotus Notes and Domino Server, IBM DB2 UDB databases, Sybase and Informix. An example is VERITAS NetBackup for Oracle. This product interfaces with Oracle RMAN and takes advantage of VERITAS NetBackup and VERITAS NetBackup media manager features. Administrators can use the VERITAS NetBackup interfaces to schedule and execute Oracle database backups in much the same manner as they can standard disk files. The VERITAS NetBackup media manager manages the storage devices and media.



Databases
- IBM DB2 UBD
- Lotus Notes and Domino Server
- Microsoft Exchange Server
- Microsoft SQL Server
- Microsoft SharePoint Portal Server
- Oracle
- SAP NetWeaver with Oracle or MaxDB/SAP DB
- Sybase
- Informix

NetBackup Agents
- NetBackup for DB2
- NetBackup for Lotus Notes
- NetBackup for MS Exchange Server
- NetBackup for MS SQL Server
- NetBackup for MS SharePoint Portal Server
- NetBackup for Oracle
- NetBackup for SAP
- NetBackup for Sybase
- NetBackup for Informix

Backup Media
- Tape
- Disk
- Optical

Figure 28: NetBackup online (hot) database backup and restore

Because VERITAS NetBackup software spans backup images across multiple tapes or disks, it can back up very large database files with any of the above methods.

MULTIPLEXING BACKUPS

VERITAS NetBackup software can run multiple backups simultaneously and stream the data to one or more devices. Backing up multiple data streams to a single tape drive is defined as "multiplexing," or "data interleaving." Backing up multiple data streams to more than one tape device is defined as "multistreaming." The backup streams can be from locally attached disks or from multiple clients over the network.

Sites can tune the configuration to the level of multiplexing desired on each device and for each schedule. Multiplexing can dramatically increase performance and allow implementation of a few fast devices, instead of many slow devices. This optimizes the use of high-speed tape devices and improves overall performance and data availability.

In conjunction with multiplexed backups, NetBackup software also restores multiplexed tape images in parallel. Please see the multiplexed restore section below for more details.

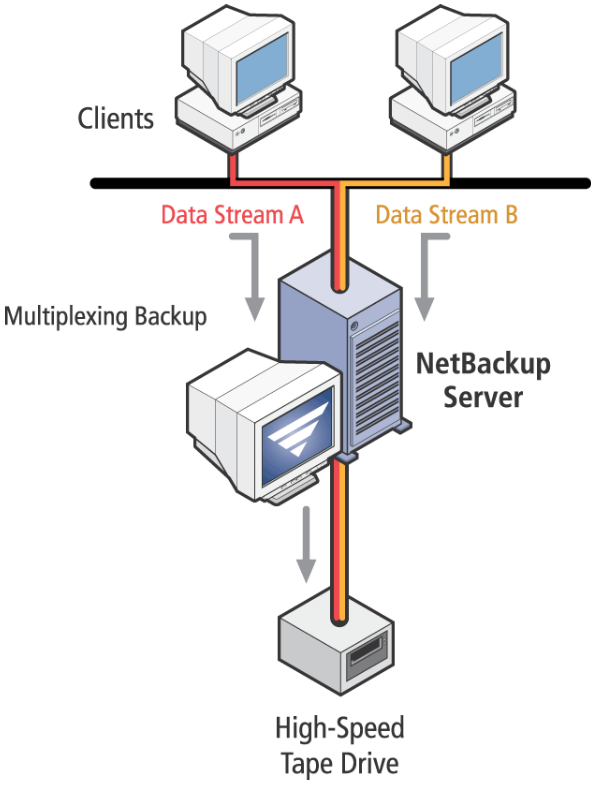
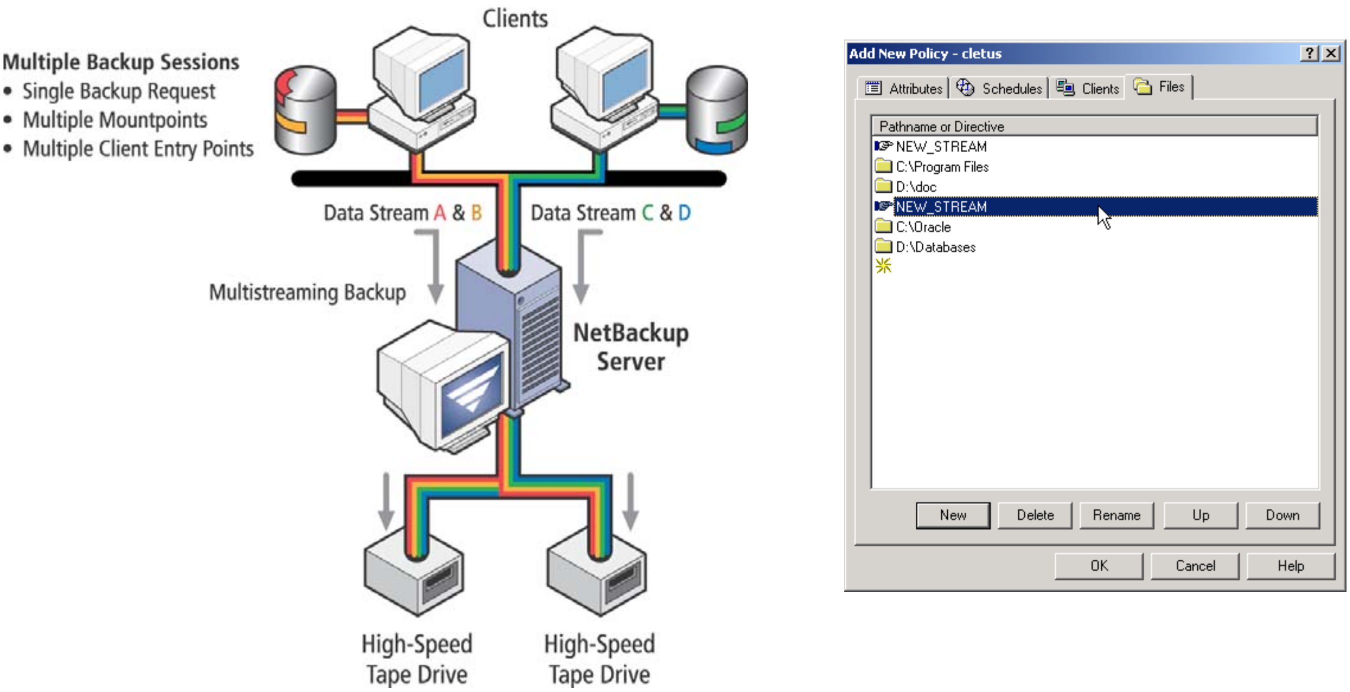


Figure 29: Multiplexed backups

AUTOMATIC MULTISTREAMING CLIENTS

A single VERITAS NetBackup backup policy can automatically create multiple, simultaneous client backup sessions and dramatically increase the performance of the backup. Parallel backup sessions are initiated based on client system mount points or individual entries (e.g. explicit or via wildcards) in the NetBackup policy file list.

The automatic multistreaming client feature can be administrator-defined to dynamically “auto discover” newly created folders and partitions on a client. An example is shown in Figure 30 below:



Pathname or Directive
NEW_STREAM
C:\Program Files
D:\doc
NEW_STREAM
C:\Oracle
D:\Databases

Figure 30: NetBackup automatic multistreaming client feature & architecture overview

COMPRESSING BACKUP DATA

VERITAS NetBackup is capable of compressing data as part of the backup operation. This action is configured with the Attributes section of a backup policy. The compression and decompression takes place on the client and its effectiveness depends on the type of data being compressed. In the right circumstances, compression significantly reduces both storage requirements and network traffic. In general, most customers find the hardware compression provided by tape devices a much simpler and efficient compression method.

BACKING UP NETWORK (CIFS/NFS) FILES

VERITAS NetBackup™ software optionally backs up files that reside on a PC network file server or on NFS file system mounted on a VERITAS NetBackup client. This is useful for backing up remote files or an unsupported client platform that has NFS files mounted on some other VERITAS NetBackup client system. See Figure 31 below for an example.

Normally it is undesirable for a client backup operation to include such files because the data transfer goes through the network protocol (IPX, TCP/IP or NFS). It is better to back up the data on the platform where the files physically reside, making backup through NFS/CIFS unnecessary.

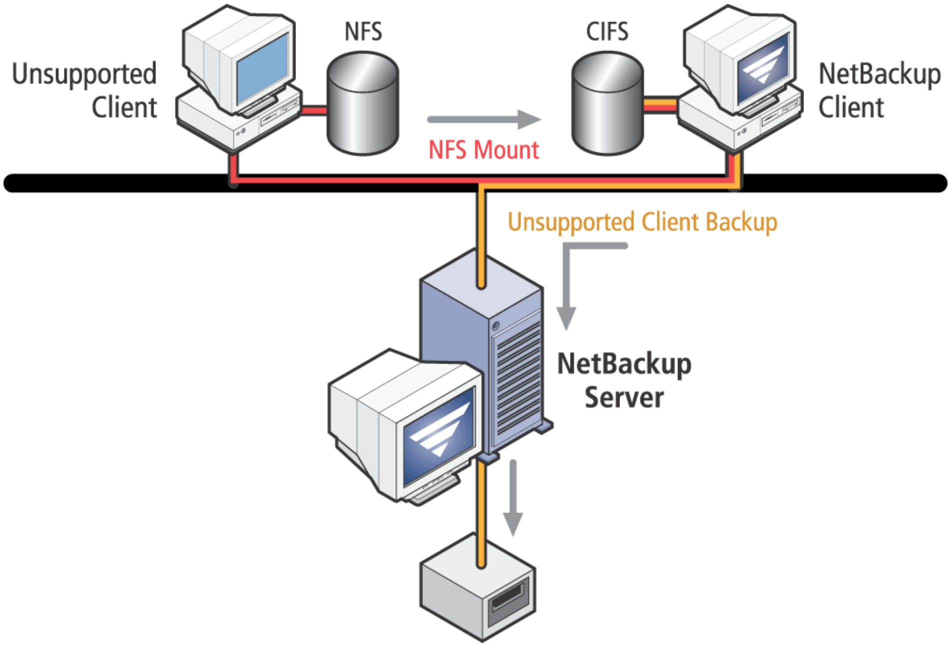


Figure 31: Using NFS mounts to back up unsupported clients

RESTORE CONCEPTS

Client users can browse their backed up files and select the ones they want to restore. When a user initiates a restore, the request passes from the client to the NetBackup master server. Once the server validates the request, the restore operation becomes fully managed by the server, which identifies the storage device and volume containing the backed up files by querying the backup catalog. The server then automatically transmits the files back to the client disk.

The process VERITAS NetBackup software uses to retrieve images from secondary storage depends on whether the storage unit is a disk file or a peripheral managed by VERITAS NetBackup EMM. In the latter case, VERITAS NetBackup assists the backup operation by handling the volume and drive allocation and mounting. When the media is mounted, the VERITAS NetBackup server reads the backed up data from the media and sends the requested portions of the image to the client.

When restoring files backed up to magnetic disk, VERITAS NetBackup software finds the image path stored in its file database during the backup operation and sends the requested portions of the image to the client. The disk manager handles the actual reading of backed up data from the disk file.

DISK BASED RESTORES

Disk based restore methods are discussed in the Disk Based Backup and Recovery section above.

MULTIPLEXING RESTORES

VERITAS NetBackup software supports the parallel multiplexed (i.e. simultaneous) restore of multiplexed backup images. To enable multiplexed restore, the tape must have been written with multiplexing enabled during the backup. Any subset of the number of “plexes” of the backup multiplexes may be restored in parallel. For example, if five backup sessions were multiplexed to the tape during the backup, any number of backup sessions up to the five could be restored in parallel with a single pass of the tape.

Multiplexed restores are especially useful for databases. Database backup performance can be optimized by multiplexing multiple sessions during the backup. However, many online database backup utilities require that if multiple backup sessions were run in parallel, they must be restored in parallel. Therefore, to enable multiplexed database backups, the backup product must support the multiplexed restore capability.

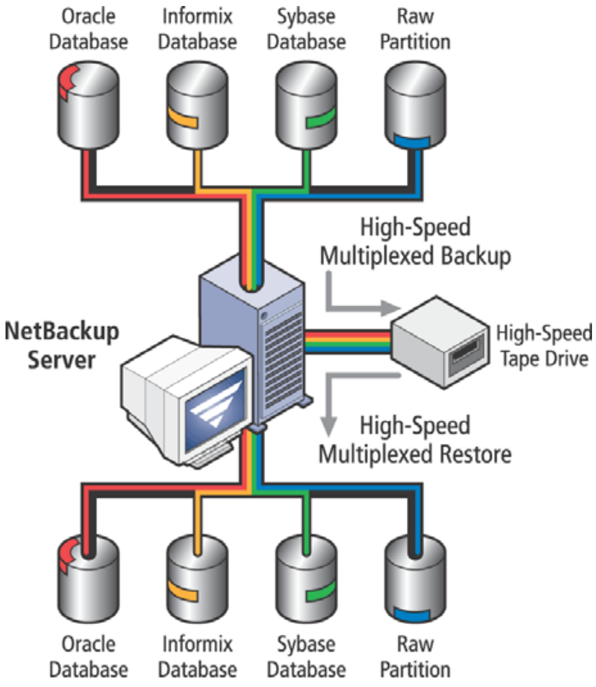


Figure 32: Multiplexed database restores

Any restore requests of a multiplexed backup image submitted inside an administrator-defined time window can be restored in parallel. For example, assume eight clients were multiplexed to a single tape during backup. If the restore of three of those clients was requested inside the administrator-defined time window, all three clients would be restored simultaneously. NetBackup software's default time window is 30 seconds.

RESTORING TO ALTERNATIVE CLIENTS

The administrator on the master server can execute an administrator-directed restore for any client, or give a user permission to browse and restore files that were backed up from another client. For example, this feature is convenient when a workstation is down and the user wants to restore backed up files to another workstation and continue working. The administrator on the master server can also direct files from the master server to any client.

SERVER INDEPENDENT RESTORES

VERITAS NetBackup™ software supports restores using a NetBackup server other than the server used to create the backup. This provides easier access to data for restores in multi-server environments, better failover and provides disaster recovery capabilities.

Restores in Multi-Server Environments

The server independent restore feature greatly simplifies operations and improves timely access to data in NetBackup environments where storage devices (e.g. tape drives or automated tape libraries) may be connected to any server in the NetBackup domain or where a large library is shared between servers (see Figure 33 below). Server independent restore applies to the following multi-server situations:

- Two or more servers are sharing an automated tape library, each with connected tape drives. When a restore is requested, one of the servers is temporarily inaccessible. Under direction of the NetBackup master server, any available server in the NetBackup domain can be used to restore the file.

- Two (or more) servers have standalone tape drives of the same type. When a restore is requested, one of the servers is temporarily inaccessible. The operator can mount the tape in a drive connected to any available server and restore the file.

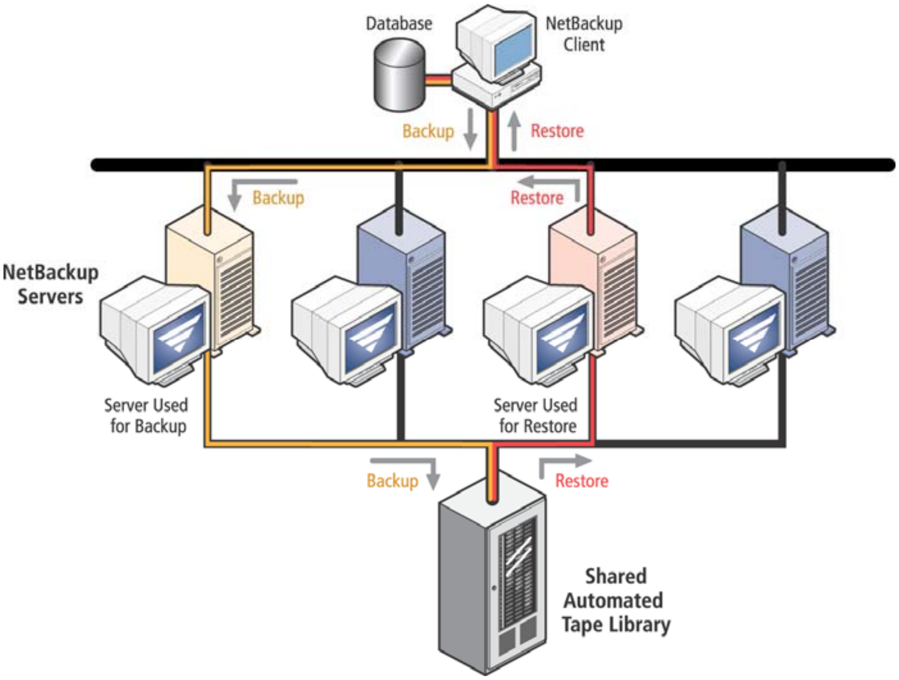


Figure 33: Server independent restores

TRUE IMAGE RESTORE

True image restore allows users to restore the most current version of their file(s). This capability can be configured on a policy-by-policy basis so that NetBackup software tracks file deletion activity and optionally prevents the restore of deleted files if a directory or file system restore is requested. Without true image recovery, files that were included in previous backups, but subsequently deleted, may also be restored by mistake.

True image restore provides installations with the option of tracking the environment as it existed at the last backup so only current data is recovered. For example, if a server needs to be recovered on a Tuesday, a combination of the last full backup tapes created on Sunday and Monday's incremental backup would be used to recover the data necessary for this server. The benefit of True image restore is that it ensures only the data that existed during the time of the Monday incremental backup will be restored to the server during recovery. The result is that all obsolete and deleted data between the Sunday full and Monday incremental is eliminated from the recovery.

In Figure 34 below, NetBackup restores 141 files, including the latest versions of 90 files that were modified. The 22 files that were deleted are ignored. Without true image recovery, NetBackup would restore 163 files.

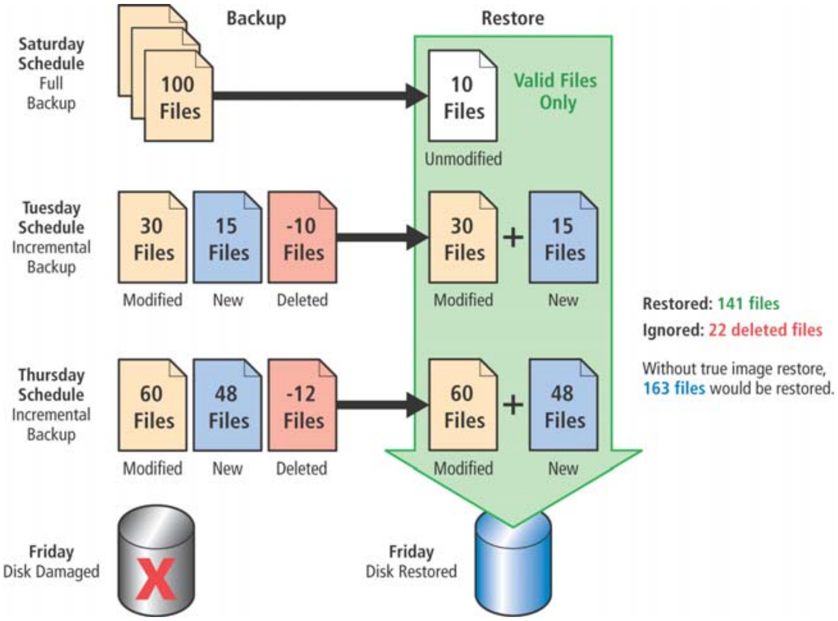


Figure 34: True image restore

The true image restore scheme used by NetBackup software keeps older true image catalogs on tape rather than on disk, avoiding the creation of large backup catalogs typical of true image backup functionality offered by other software vendors.

Backup/Restore of Moved Directories and Files

The true image restore feature enables administrators to check that moved, renamed or newly installed files and directories are detected and backed up during incremental backups by comparing the new file and directory names to those in the previous full or incremental backup. A catalog of the previous full or incremental backup is saved on the NetBackup client.

Some client disk space is required to store partial backup catalogs. This is an optional feature since additional system resources are required.

VERITAS NETBACKUP BARE METAL RESTORE OPTION

A full server recovery where the root volume or operating system is non-operable presents serious challenges to systems administrators. In such cases, a bare metal restore must be executed to rebuild the machine configuration and provide the necessary operating system components to allow NetBackup software to restore the appropriate applications and data. There exist a variety of techniques and tools to address this problem, but all have significant deficiencies.

Manual recovery procedures are very time consuming. The user must first reinstall a machine's operating system and applications, restore the data and then fix the configuration and reconcile any differences between the reinstalled and restored pieces. It can take days to try to recover a machine this way, and in the end it is often impossible to completely recover the machine. In addition, there are many opportunities for error along the way. Many of these errors are subtle and can take additional days to discover, troubleshoot and rectify.

Certain tools exist that attempt to shorten full server recovery time and eliminate human error though automation. Until recently, these tools represented the only solutions available to perform full server recovery following a catastrophic system failure. But these tools have shortcomings as well. They are platform specific and require skilled administrators with specialized skills, thereby preventing the deployment of common tools and processes to lower costs and reduce human error. These traditional techniques wasted storage, bandwidth, and human effort by requiring special redundant backups or unique system images for use during recovery. Because these techniques were inefficient and cumbersome to administer, these special backups and images were often out of date and not very useful during system recovery. As a result, when restoring a machine from the special backup or image, that backup or image may be completely out of sync with the data on the NetBackup server. There was no way to ensure a coherent recovery of the system when you were trying to patch together data that was backed up at different times by different applications.

With the VERITAS NetBackup Bare Metal Restore option, NetBackup software gains an essential supplemental capability to perform heterogeneous, automated, full system recovery. Using the NetBackup Bare Metal Restore option enables:

- A simplified, automated, error-free recovery.
- Common user interface (NetBackup Administrative Console).
- A single full server recovery solution for all major enterprise platforms that leverages your existing NetBackup infrastructure.
- Reduced cost through the use of automation, centralized administration, common tools and procedures, and lower-cost human skills; elimination of redundant resource consumption, and increased parallelism of system recovery.
- Leverages the NetBackup internal infrastructure
    - Ports
    - Security
    - Catalog
    - Logging

The result is that the NetBackup Bare Metal Restore option reduces server recovery to a simple two-step process:

- Issue the "prepare to restore" command, either via a browser-based NetBackup Bare Metal Restore GUI or command line.
- Reboot the system.

NetBackup Bare Metal Restore option performance efficiencies are achieved through intelligent separation of functions. The main functions provided by NetBackup Bare Metal Restore option include:

- Automatically saving each protected system's "meta-data" - including disk configuration and partitioning information as well as TCP/IP information - on a regular basis for use during system recovery.
- Supporting a recovery infrastructure that provides all the files and services necessary to perform system recovery, including the ability to perform diskless network booting, temporary OS installation and disk configuration.
- Dynamically generating a customized recovery procedure. This is a program built to order for the specific system being recovered that is not created until the prepare to restore command is issued.

NetBackup Bare Metal Restore option executables are installed on each protected system. Bare Metal Restore option software's primary function is to save an up-to-date snapshot of the system's configuration each time a scheduled backup executes. This snapshot is referred to as the client's "meta-data". The meta-data is required to rebuild the machine during Bare Metal Restore system recovery. On the Windows platform, the Bare Metal Restore client is also responsible for the creation/modification of the SRT and creating the bootable floppy disk. The bmrsavecfg program saves the client's current meta-data immediately prior to each scheduled backup. The bmrsavecfg program is integrated with Bare Metal Restore scheduled backups via bpstart_notify.

NetBackup Bare Metal Restore option software supports full server recovery on HP-UX, IBM AIX, Sun Solaris, Windows and Linux. For up to date support information, please go to http://support.veritas.com/ .

For more in-depth information on the NetBackup Bare Metal Restore option software, please reference the NetBackup Bare Metal Restore white paper.

SECURITY

Storage management applications have often been characterized as the biggest security loophole in a secure data environment. Once the data leaves the confines of the physical system environment by way of a backup or data migration, the data security policies and procedures often do not follow.

VERITAS NetBackup™ software addresses security concerns in the enterprise storage management environment by providing customers with a wide range of security options. These include authentication, authorization, data encryption and auditing. Each can be tailored to meet a customer's specific needs. Data can be encrypted before it is sent across the network and/or before it is stored on tape.

AUTHENTICATION

VERITAS NetBackup authenticates via a peer-to-peer protocol between NetBackup master servers, remote servers and clients to validate that systems are what they say they are and protect against "spoofing." The authentication takes place after a NetBackup connection has been established, but before any NetBackup transactions have taken place.

For NetBackup, the standard authentication method is a one-time password (i.e. challenge/response) mechanism based on the U.S. Navy's OPIE protocol. The one-time password method was chosen because it is secure, portable and exportable.

AUTHORIZATION

VERITAS NetBackup protects data from unauthorized access through the use of secure client hosts to restrict client-server communications and administrator-imposed restrictions on restore operations.

Users do not have direct access to the volumes containing their backed up files and cannot choose their own media volumes. The VERITAS NetBackup server, not the user, chooses the secondary storage media. In addition, VERITAS NetBackup media manager allows only VERITAS NetBackup software to have access to these volumes and imposes access control to protect the backed up files from unauthorized viewing or use by other applications.

Under normal conditions, VERITAS NetBackup software prohibits users from viewing or restoring other people's files. By default, VERITAS NetBackup software enforces normal file viewing and restoration restrictions in which client users may view or restore only those files that they personally backed up or archived from that client.

Administrators, however, have the flexibility to modify these restrictions to meet special site requirements. The administrator may relax file access restrictions by giving designated clients on a server access to backup or archive images created on any other designated clients. For minimum security, the administrator can disable all restrictions, permitting access by any client.

Typically, the NetBackup administrator has administrative — or root — privileges. For flexibility, however, NetBackup supports the creation of a set of non-administrative (i.e. root) users who have full NetBackup privileges, from creating or modifying backup policy to managing backup and restore activities. NetBackup software also supports restricting an administrative (i.e. root) user from administering NetBackup software.

With the introduction of a feature known as **Access Control**, NetBackup now has even further security mechanisms for all users of product. Access Control allows NetBackup administrators to protect their NetBackup configuration by enabling Access Control to define three factors that control or restrict access to NetBackup:

- Who may access NetBackup: Accomplished by defining users and user groups.
- What functions a user group can perform: Accomplished by assigning users to various user groups.

- What resources a user group may manage.

For the purpose of authentication, Access Control can work in conjunction with following:

- Windows Platform- Primary Domain Controller or Active Directory
- UNIX Platform- NIS/NIS+, UNIX passwords

ENCRYPTION

NetBackup software protects critical data from unauthorized access and tampering while in transit, as well as when it resides on backup media. NetBackup software performs the data encryption on the client, transfers the data across the network and stores it on tape in the encrypted format. On restores, the data is read from media and transferred across the network to the client before decrypting.

The NetBackup Encryption option user has the ability to encrypt data using 128-bit or 256-bit OpenSSL ciphers as well as 40-bit DES or 56-bit DES.

The encryption level needed can be set during the installation process and all encryption code is delivered with this single option.

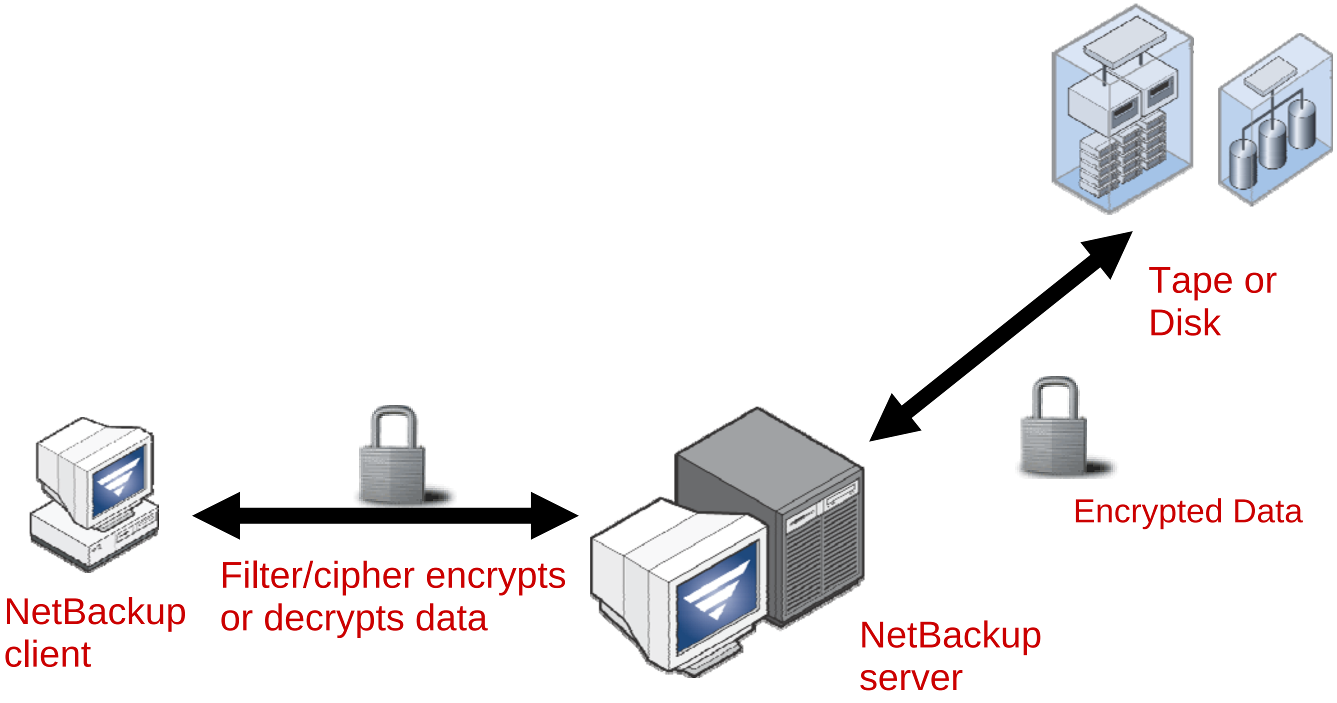


Figure 35: NetBackup software data encryption

DEVICE AND MEDIA MANAGEMENT

Enterprise Media Manager

The Enterprise Media Manager (EMM) consolidates all media and device information into a single relational database. When volumes are added, they are recorded in the relational database. The NetBackup resource broker can then query the database in order to allocate storage units, drives (e.g., including drive paths), and media. The restructuring allows for improved performance, scalability and manageability of NetBackup media and devices. The following table lists some of the changes starting with NetBackup 6.0.

NetBackup Catalog

NetBackup keeps a catalog with information that correlates backups to the volume where they are stored. NetBackup refers to the catalog when it needs a volume for a backup or restore. If the catalog does not contain suitable volume for a backup job, NetBackup has media manager assign one. In this manner, the catalog is populated as NetBackup uses new media for backups.

When the retention period has ended for all backups on a volume, NetBackup deletes the volume from the catalog. NetBackup then sends a request to Media Manager to unassign the volume so it is available for later reassignment.

Volumes for backups of the NetBackup catalogs are a special case and do not appear in the NetBackup catalog.

These volumes are typically assigned to the Catalog Backup volume pool so you can find them in case the NetBackup catalog is damaged. These volumes are unassigned only if you delete them from your catalog backup settings.

Alternatively, you can locate media for catalog backups using the physical inventory utility. It may take significant time for each tape to be mounted so its recorded label can be read.

For more in-depth information on the NetBackup catalog, please reference the NetBackup Scalable Data Protection for the Enterprise white paper.

BASIC VOLUME MANAGEMENT PROCESS

The three main elements of VERITAS NetBackup Enterprise Media Manager are as follows:

- **Robot Management** — Supports robotic secondary storage devices.
- **Device Management** — Lets you share secondary storage devices among different users and applications.
- **Media Management** — Tracks the location of all removable media and secondary storage devices in your system and gathers media usage statistics.

The term volume, as used by VERITAS NetBackup software, refers to the physical storage media on which VERITAS NetBackup software stores its backups, such as tape or optical disk. The device manager controls the actual mounting of volumes on the tape or optical storage devices in response to requests from VERITAS NetBackup software or other products. These requests specify both the volume name and device density.

VERITAS NetBackup uses the device manager gets volume information from the relational database. If the request involves a robot, this information includes the specific robot that has the volume and the slot location of the volume in the robot. The device then issues a mount command to the robotic daemon controlling that robot, which automatically mounts the specified volume and returns control to the VERITAS NetBackup software. No operator intervention is required, provided the required volume is physically in the robot.

If the volume is not in the tape library, the device manager alerts the operator by sending a mount request to the NetBackup console. The operator then finds the volume and inserts it into the library so the operation can proceed. Bar-code verification is also supported for robots with bar-code readers. This provides an extra measure of confidence that the correct volume is being mounted.

With a standalone drive, VERITAS NetBackup software attempts to use the media that is in the drive. If the drive does not contain media, the device manager alerts the operator by sending a mount request to the NetBackup console. The operator then finds the volume, mounts it manually and assigns it to the request.

The VERITAS NetBackup EMM allocates a previously unassigned volume to VERITAS NetBackup software whenever a new volume is required for either a standalone or robotic drive. Volumes allocated to VERITAS NetBackup come from the volume pool designated for the specific backup files, which by default is the NetBackup volume pool. The term volume pool refers to a distinct set of volumes that are assigned for a specific use.

In addition to assigning volumes, the VERITAS NetBackup EMM tracks the location of both online and offline volumes and keeps this information in the volume database.

SHARED STORAGE OPTION (DYNAMIC DRIVE SHARING)

The VERITAS NetBackup Shared Storage Option software allows individual tape drives, either standalone or in a robotic library to be dynamically shared between multiple NetBackup servers. Drives can be dynamically allocated across NetBackup servers as backup/restore operations dictate. This software option requires appropriate hardware connectivity, such as a SCSI multiplexer or fiber switch/hub Storage Area Network (SAN). If the robotic control is SCSI-based, one host controls the robotics (see the “Sharing Tape Libraries” section below).

Shared Storage Option for NDMP allows for the sharing of tape drives among media servers and NDMP-NAS devices. This feature supports multiple paths to tape drives for redundancy.

Figure 36 below diagrams an example of a shared drive configuration. Multiple NetBackup servers (e.g. master servers or media servers) are grouped around one or more multi-drive libraries connected by a Fibre Channel switch. During setup, the system administrator designates which drives are to be shared among NetBackup servers and/or NDMP hosts. Drives not designated as shared drives are dedicated to a single server.

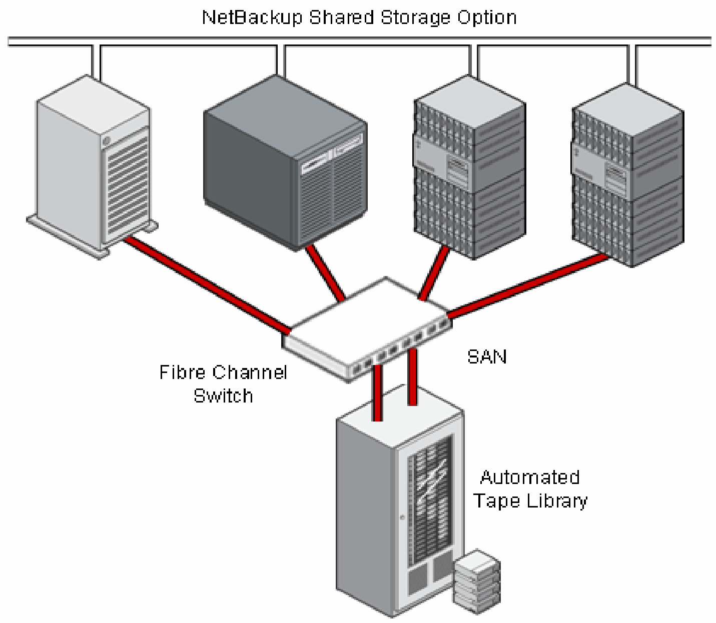


Figure 36: Sharing tape drive resources between NetBackup servers using the NetBackup Shared Storage Option

SHARING TAPE LIBRARIES

The VERITAS NetBackup EMM enables multiple backup servers to share a multi-drive tape library. One NetBackup server acts as the “robotic control host,” and other NetBackup server’s request tape mount and dismount services from the control host. In this type of configuration, each NetBackup server maintains dedicated data paths to maximize performance without sacrificing the cost-effectiveness and economies of scale of large tape libraries.

MANAGING ROBOT INVENTORY

Managing the contents of robots is a critical task and can be very difficult when a site has a large number of robotic volumes. VERITAS NetBackup media manager provides options designed to make this task much easier by allowing an administrator to:

- **Automatically populate the volume database for a new robot**
  In a new configuration, the administrator can load a robot with new media and then have VERITAS NetBackup EMM automatically add the volumes to its volume database. If bar codes are being used, VERITAS NetBackup EMM automatically registers the new media according to the bar codes. By defining rules based on bar codes, the administrator can have the VERITAS NetBackup EMM initialize volume database entries with specified values for volume pool, media type, maximum number of mounts and volume description.
- **Update the volume database after changing the contents of a robot**
  After adding or removing volumes, the administrator can have the VERITAS NetBackup EMM physically inventory a robot and automatically update the volume database so it coincides with the inventory results. When volumes are moved in or out of the robot, VERITAS NetBackup EMM updates the database accordingly.

The administrator can also generate reports that show:

- What is physically in a robot?
- Discrepancies between what is physically in a robot and what is shown in the volume database.

SCRATCH POOLS

The VERITAS NetBackup EMM enables administrators to configure and enable scratch pools. When applications such as NetBackup need additional media, they can obtain new media from the scratch pool. Scratch pools can be local to a single storage unit such as a library, or be configured across multiple storage units. This allows the administrator to add all new tape volumes to the scratch pool, rather than statically assigning new media for use by specific applications. NetBackup software can also be configured so that when the backup images on a tape that originated from the scratch pool expire, the tape will be automatically returned to the scratch pool for reuse.

SPANNING VOLUMES FOR LARGE IMAGES

When a backup image is too large to fit on a single volume, VERITAS NetBackup software fills each volume to capacity and then automatically spans the image to another volume. This makes the most efficient use of media and is especially useful when backing up large images that are commonly encountered with databases. If spanning volumes is not desired, the administrator can disable this feature if necessary.

TRACKING MEDIA AGE AND NUMBER OF MOUNTS

Because the possibility of media failure increases with age and use, VERITAS NetBackup EMM keeps statistics on how old the media is and how often it has been mounted. The administrator can choose to expire the physical media based on date or a specified number of mounts.

MEDIA OVERWRITE PROTECTION

Many environments have media written by applications other than VERITAS NetBackup. In these instances, it is important that the old media is not accidentally overwritten. If the media is overwritten, the data is lost and cannot be recovered. To prevent this, VERITAS NetBackup software provides overwrite protection for a number of different formats, including tar, CPIO and ANSI labeled.

By default, VERITAS NetBackup software refuses to overwrite a protected format. It is possible to override this protection in case it is necessary to reuse the media for NetBackup backup images. This option can be useful when phasing over to NetBackup from an application that uses one of these protected formats.

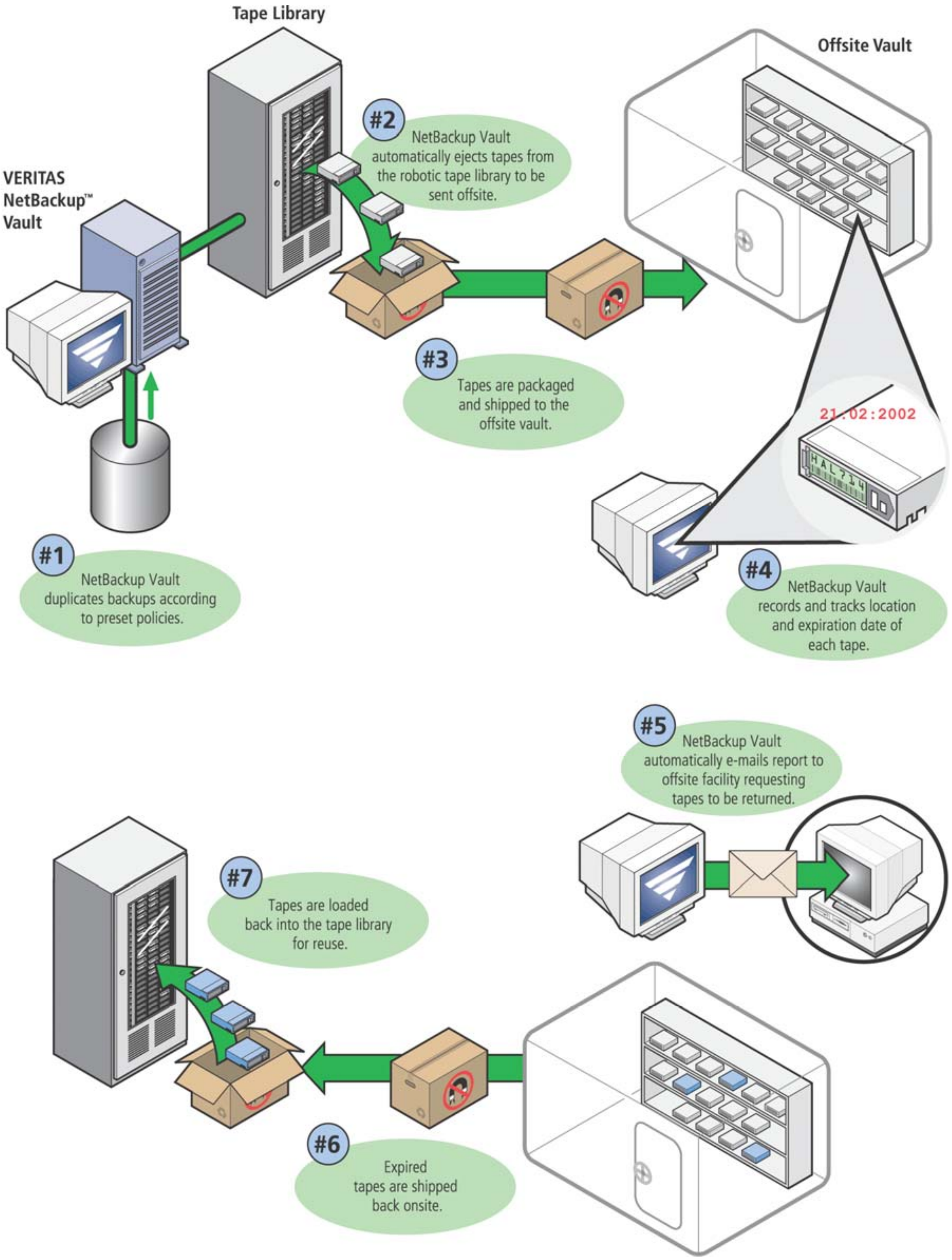
VERIFYING MEDIA

A verification option allows the administrator to read NetBackup media and compare its contents to the online catalog of information in VERITAS NetBackup.

VERITAS NETBACKUP VAULT

Managing offsite tapes for disaster recovery can be a cumbersome, manual process (see Figure 37 below). While a basic spreadsheet can be used. However, if your vault and disaster recovery plans mandate that hundreds or thousands of tapes be moved weekly between your primary site and your vault, this process can quickly become a logistical nightmare. To solve this problem, NetBackup Vault software simplifies and automates the life cycle management of offsite tape media. The following are key functions of the NetBackup Vault software:

- Ejection of tape media
- Assigning of tape media slot IDs at offsite vault
- Monitoring tape retention periods so expired media may be brought back to the primary site for reuse.
- Creation of vault reports (e.g. media going offsite, media coming onsite, detailed media reports) for managing offsite media
- Iron Mountain Reporting Capability
    - Support for Iron Mountain Electronic Format Report
    - Includes Picking List, Distribution List, Inventory Report and the Recovery Report
- Report consolidation
- Distribution granularity
- Non-Vaulted Images Report
- Vault Lost Media Report
- Container Inventory Report
- Queue Vault Jobs



#1 NetBackup Vault duplicates backups according to preset policies.

#2 NetBackup Vault automatically ejects tapes from the robotic tape library to be sent offsite.

#3 Tapes are packaged and shipped to the offsite vault.

#4 NetBackup Vault records and tracks location and expiration date of each tape.

#5 NetBackup Vault automatically e-mails report to offsite facility requesting tapes to be returned.

#6 Expired tapes are shipped back onsite.

#7 Tapes are loaded back into the tape library for reuse.

Figure 37: Typical offsite vaulting process

IMPORTING MEDIA

An import option allows administrators to import VERITAS NetBackup™ database information from VERITAS NetBackup media or backups written to Disk Storage Units that have expired or were created on another master server. Some examples of using this feature are to move backups or archives to a master server at another location or to regenerate the NetBackup catalogs from regular backup media. This is normally not required because of the special processes that NetBackup software provides for backing up its databases, but it is an extra measure of insurance against possible data loss.

ADMINISTRATION AND USE

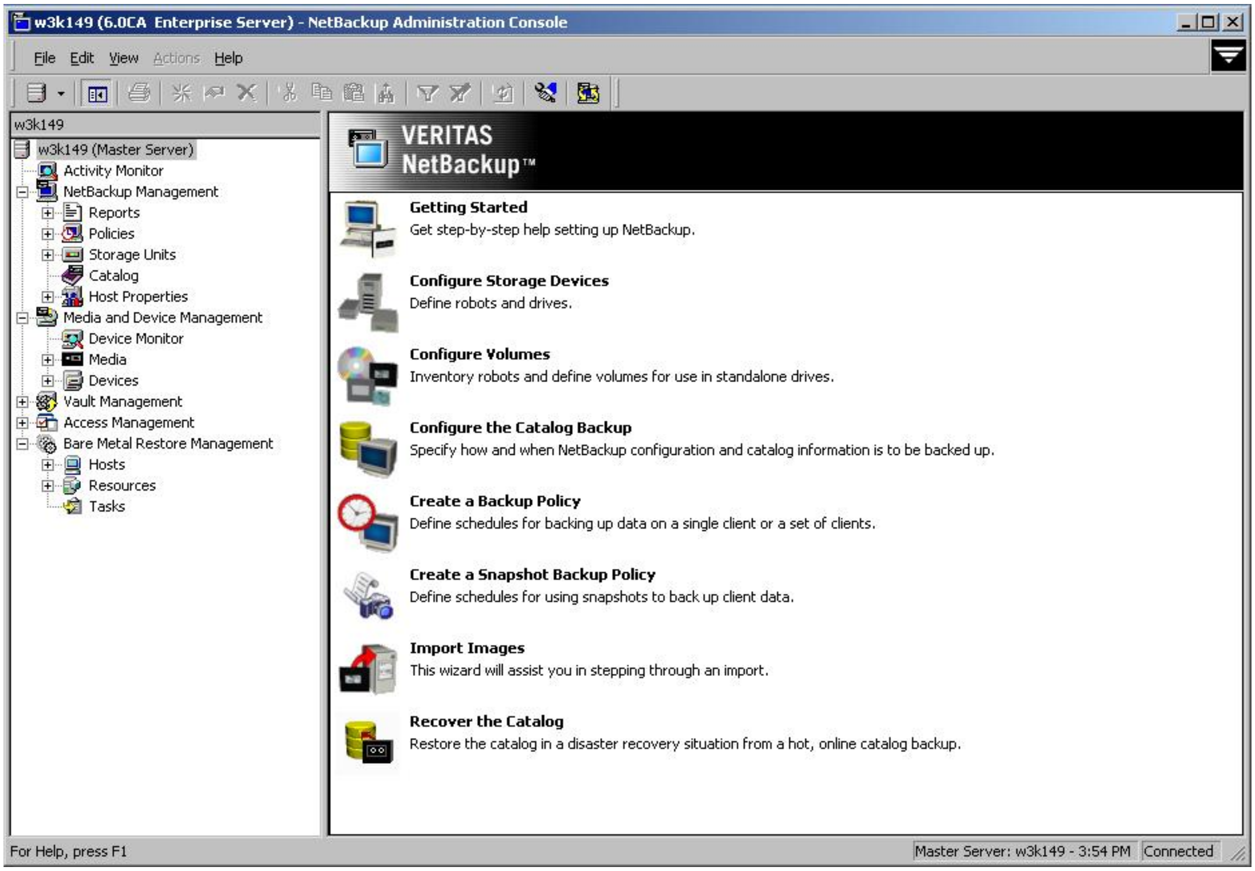
VERITAS NetBackup and VERITAS NetBackup EMM provide a comprehensive and logically designed set of interfaces that make it easy to perform all required administration, backup or restore tasks. There are GUI (Graphical User Interface) and command line versions of most interfaces.

The graphical user interfaces provide the greatest ease of use with icons, pull-down menus and full mouse support. These interfaces are Java- or Windows-based, depending on the platform. Graphical wizards assist in the installation and configuration of devices, media and policies.

In addition to what can be done from the GUI and menu interfaces, many operations can be started from the command line, enabling the use of scripts if desired by the NetBackup user.

ADMINISTRATOR INTERFACES

The administrator interfaces provide access to all information necessary to configure and manage VERITAS NetBackup and VERITAS NetBackup EMM. You can perform this administration from a single point (see Figure 38 below), regardless of the number of servers or clients in the NetBackup software configuration.



Getting Started
Get step-by-step help setting up NetBackup.

Configure Storage Devices
Define robots and drives.

Configure Volumes
Inventory robots and define volumes for use in standalone drives.

Configure the Catalog Backup
Specify how and when NetBackup configuration and catalog information is to be backed up.

Create a Backup Policy
Define schedules for backing up data on a single client or a set of clients.

Create a Snapshot Backup Policy
Define schedules for using snapshots to back up client data.

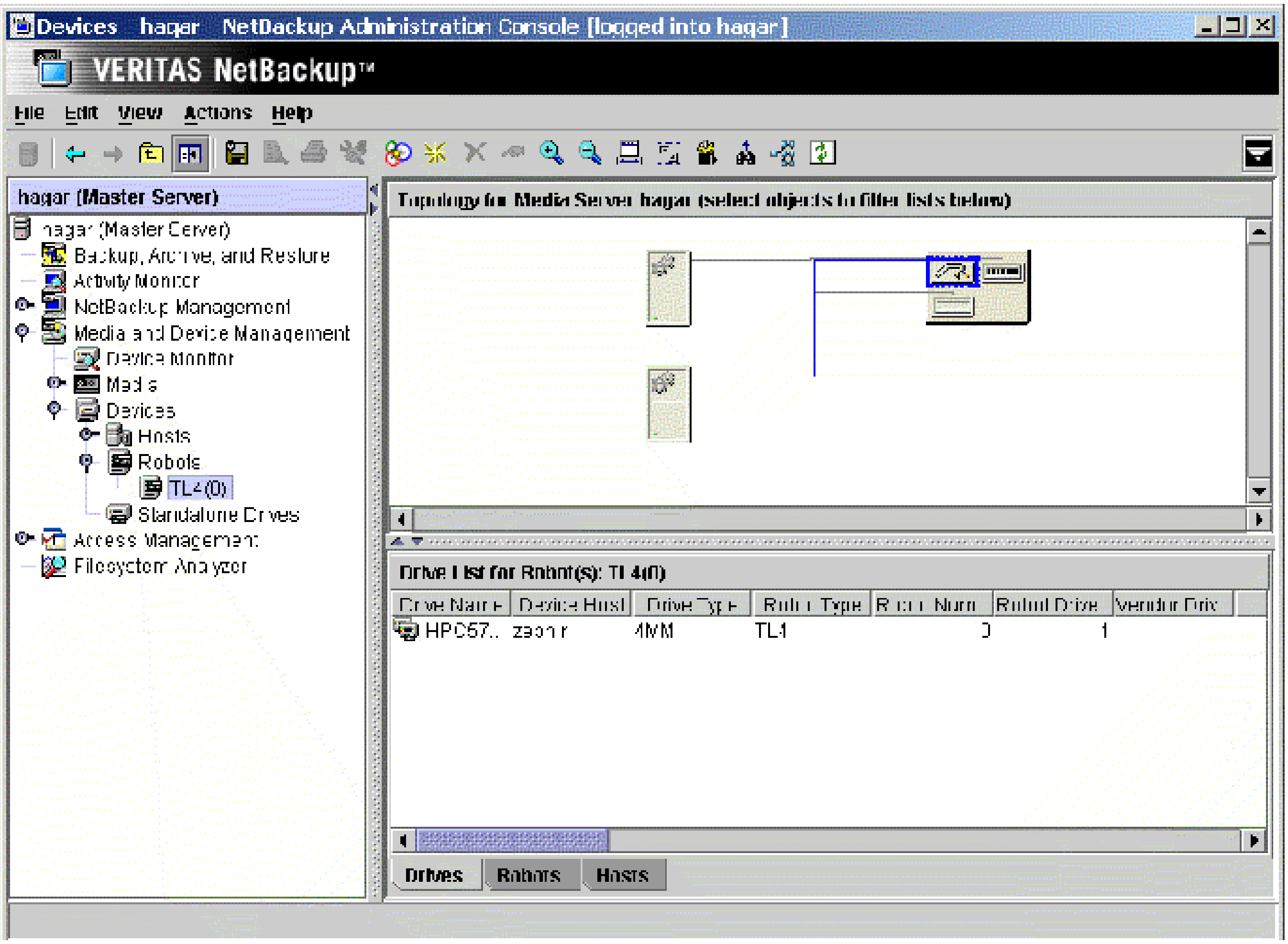
Import Images
This wizard will assist you in stepping through an import.

Recover the Catalog
Restore the catalog in a disaster recovery situation from a hot, online catalog backup.

Figure 38: Centralized administration via the NetBackup Administration Console

The VERITAS NetBackup administration console consolidates NetBackup software control via both graphical tools and wizards that are used for NetBackup software configuration. From this screen administrators can create backup policies or define storage units. The console presents a consistent, easy-to-use window for administering data protection activities for NetBackup domains. To change from domain to domain (i.e. master server to master server), simply go to the File menu and select “Change Server”, or go directly to the Change Server icon on the console toolbar.

The VERITAS NetBackup EMM also has graphical user interfaces for managing its devices and media. Figure 39 below shows the screen for managing devices. The administrator uses this screen to check and alter the status of devices. The menu version shows similar information.



Drive List for Robot(s): TL4(0)

Drive Name	Device Host	Drive Type	Robot Type	Robot Num	Robot Drive	Vendor Driv
HPC57..	zeon r	4MM	TL4	0	1	

.

Figure 39: NetBackup Administrator Console screen for managing storage devices

Other screens allow the NetBackup administrator to configure media for use under VERITAS NetBackup media manager or to perform other tasks related to VERITAS NetBackup EMM configuration and administration.

A site administrator can even define custom menus and menu commands for the administrator graphical user interfaces. These menus will appear on the main window of the interface and contain whatever commands the administrator has added to them.

Several wizards have been designed to step novice users through common setup and configuration tasks. These wizards simplify and accelerate the process of adding devices, media or backup policies, and reduce the likelihood of error.

USER INTERFACES

Users can initiate backups, restores and archives from their client workstation without logging into the server and without administrator intervention. Figure 40 below shows the functionality that the NetBackup user can initiate from the NetBackup user interface:

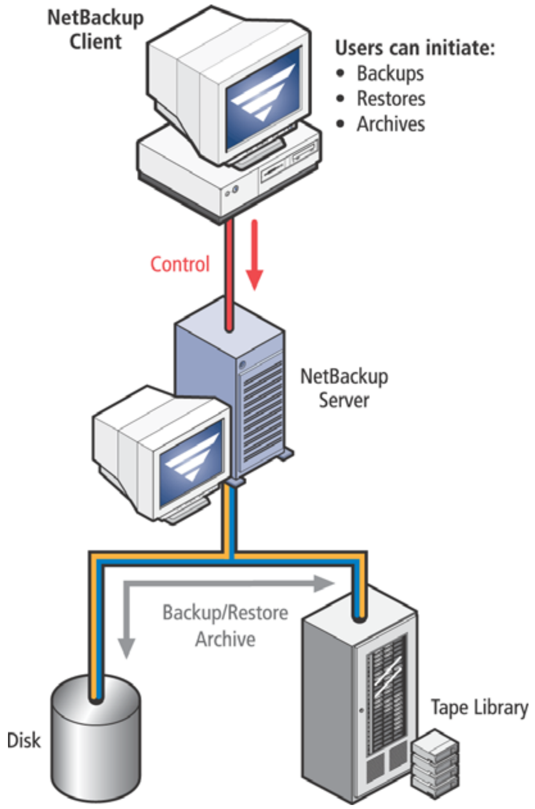
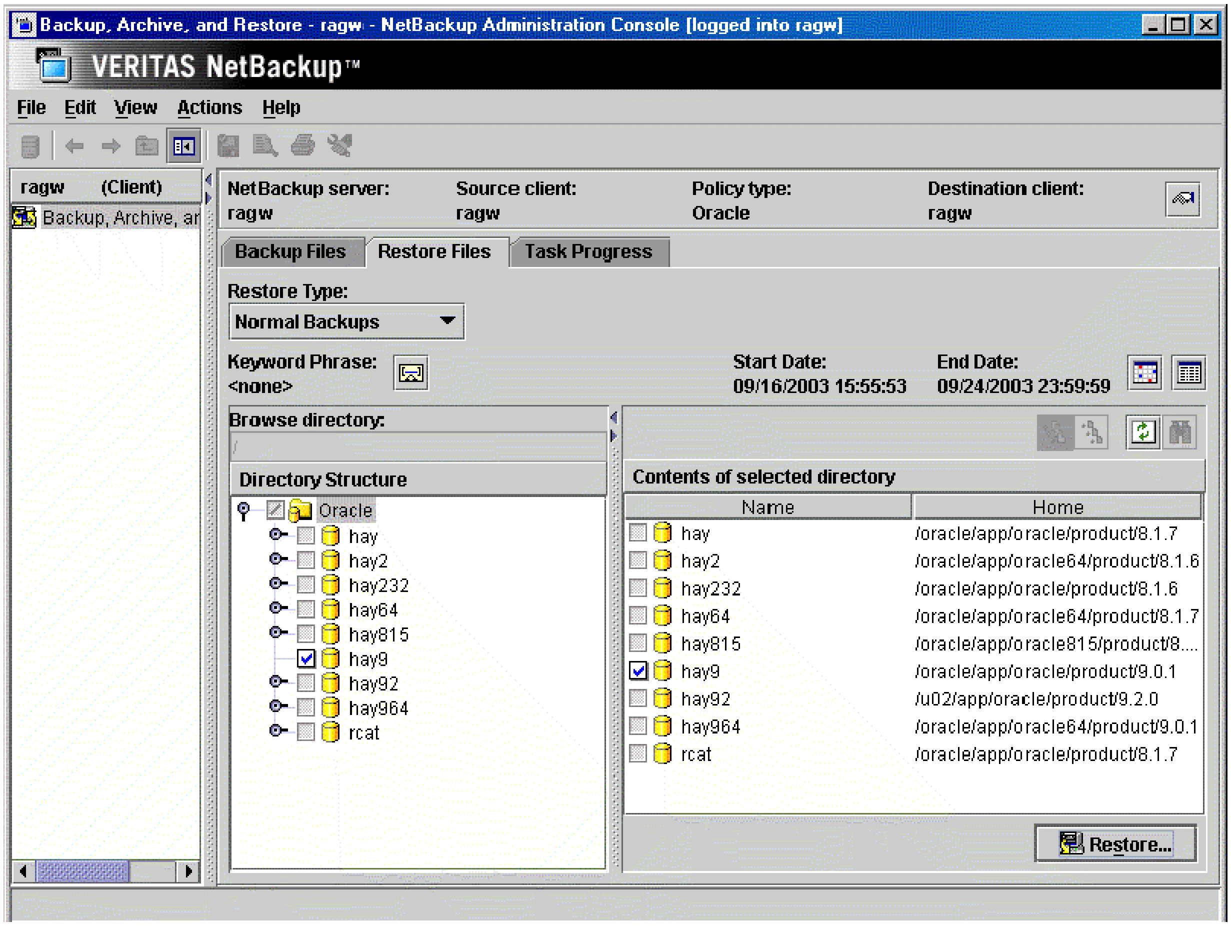


Figure 40: NetBackup client backup initiated from the NetBackup user interface

Figure 41 below shows a typical user interface screen for VERITAS NetBackup software. This example shows the restore screen where users can scroll through the list of backed up or archived files and select those to be restored to the client disk. A menu version of this interface provides the same functionality from a character-based terminal. In addition, a command line interface enables users to create their own shell scripts to perform client-directed operations.



NetBackup server: ragw
Source client: ragw
Policy type: Oracle
Destination client: ragw

Restore Type: Normal Backups

Keyword Phrase: <none>

Start Date: 09/16/2003 15:55:53
End Date: 09/24/2003 23:59:59

Browse directory: /

Directory Structure:

- ☑ Oracle
  - ☐ hay
  - ☐ hay2
  - ☐ hay232
  - ☐ hay64
  - ☐ hay815
  - ☑ hay9
  - ☐ hay92
  - ☐ hay964
  - ☐ rcat

Contents of selected directory

	Name	Home
☐	hay	/oracle/app/oracle/product/8.1.7
☐	hay2	/oracle/app/oracle64/product/8.1.6
☐	hay232	/oracle/app/oracle/product/8.1.6
☐	hay64	/oracle/app/oracle64/product/8.1.7
☐	hay815	/oracle/app/oracle815/product/8....
☑	hay9	/oracle/app/oracle/product/9.0.1
☐	hay92	/u02/app/oracle/product/9.2.0
☐	hay964	/oracle/app/oracle64/product/9.0.1
☐	rcat	/oracle/app/oracle/product/8.1.7

Figure 41: NetBackup Backup, Archive, and Restore user interface window for restoring files

INSTALLATION

It is possible to install and configure VERITAS NetBackup™ software on standalone systems or on heterogeneous client/server networks supporting thousands of clients. The administrator first installs software on the master server, then on media servers if required to protect the user's environment, and then on the clients where the data resides.

Windows InstallShield wizards or installation scripts automate the entire install process. When the software is installed, the administrator configures VERITAS NetBackup software by using the administrator interfaces.

For UNIX clients, software is initially read into the server and subsequently pushed to the clients across the network. This greatly speeds the installation process because there is no need to install client software from CD on individual clients. The administrator installs software upgrades in the same manner, quickly and easily across the network. Windows clients are installed from a Windows domain or AD server or CD. PC and Macintosh client software is quickly and easily installed on each client via CD. It is also possible to install the software so LAN file servers can share NetBackup program files with its clients.

CONFIGURATION

During initial configuration, the administrator can start with the NetBackup default options, which were carefully chosen by VERITAS to meet most of the requirements for typical installations. From this point, well-designed administrator interfaces and wizards along with online help and descriptive product documentation make it easy to customize the setup for a specific site.

The main tasks involved in completing the configuration are:

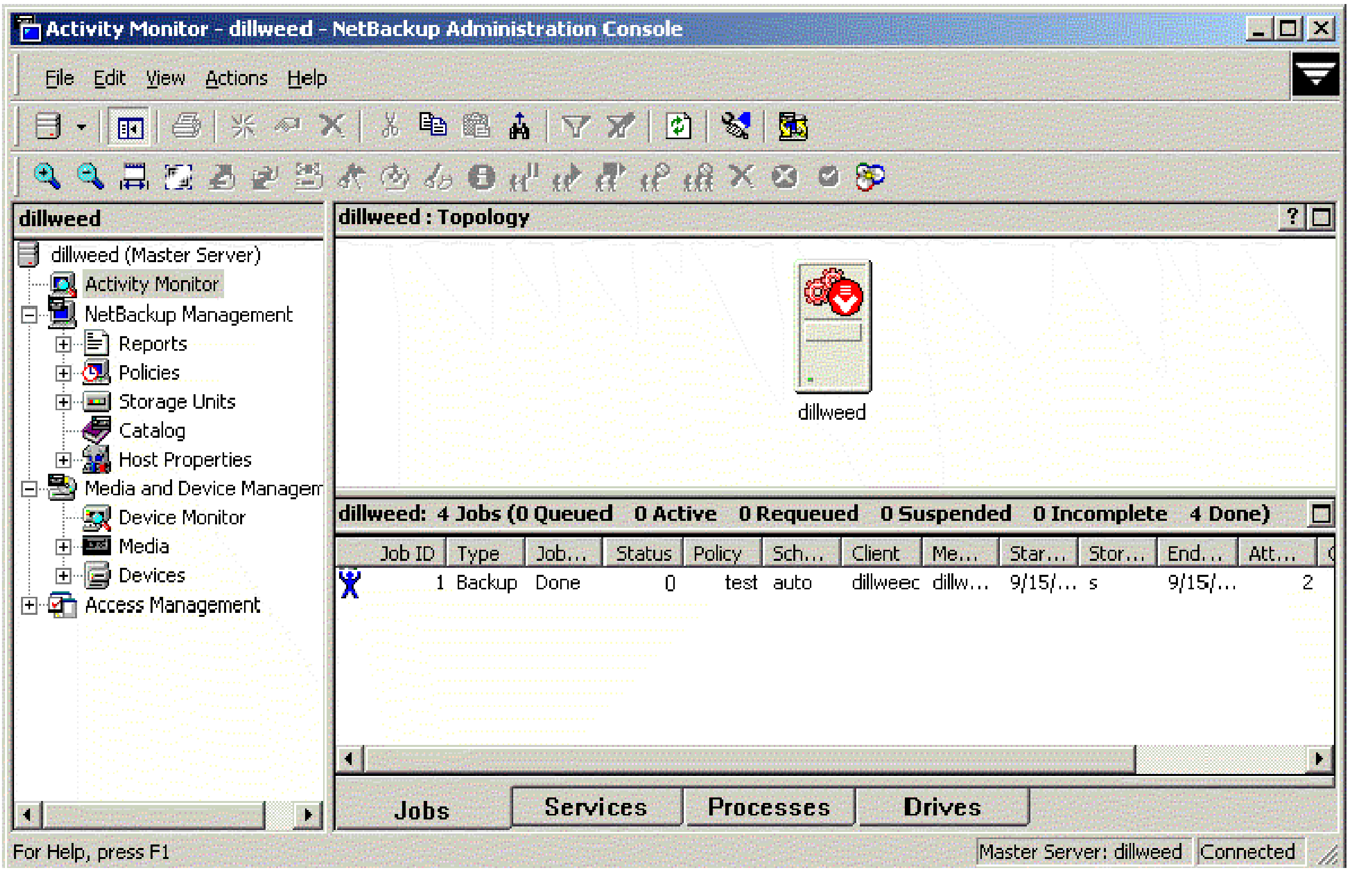
- Identify the storage devices available to VERITAS NetBackup EMM. The serialized hardware is automatically discovered by the NetBackup software
- Register media for use as volumes by VERITAS NetBackup EMM
- Define the type and density of devices that will be in the storage units
- Define VERITAS NetBackup policies including:
    - Clients in each policy
    - Files to back up on the clients
    - Backup schedules

The interfaces provide change options that make it easy for the administrator to modify the values set during the initial configuration. Tape drives and robotic devices are automatically discovered as long as the hardware supports device serialization. Most current hardware today supports device serialization.

ACTIVITY MONITORING

The VERITAS NetBackup activity monitor allows administrators to monitor progress and status of backup, restore, duplication and archive jobs. Figure 42 below shows the job window with statistics about a selected job. Job control is also provided so an administrator can cancel jobs if necessary, which is useful in correcting problem situations such as if a job is hung or too many jobs are being processed by NetBackup at one time.

In some instances, it may be desirable to produce a report about current and completed jobs without using the Job Monitor interface. The administrator can do this by executing a command from the system prompt or from a custom script.



dillweed: 4 Jobs (0 Queued 0 Active 0 Requeued 0 Suspended 0 Incomplete 4 Done)

Job ID	Type	Job...	Status	Policy	Sch...	Client	Me...	Star...	Stor...	End...	Att...
1	Backup	Done	0	test	auto	dillweec	dillw...	9/15/...	s	9/15/...	2

Figure 42: The NetBackup activity monitor screen

SUPPORTED HARDWARE AND SOFTWARE

The list of hardware and software platforms supported by VERITAS NetBackup software and the peripheral storage devices supported by VERITAS NetBackup EMM is continually growing. For questions about a particular client or server platform, operating system or peripheral device, refer to www.support.veritas.com or contact your VERITAS Software sales representative or reseller.

SUMMARY

VERITAS NetBackup™ software brings the same level of storage management support to the world of open systems found in traditional centralized mainframe installations. It is possible to fully automate file backup and archive schedules across entire networks.

Client users are more productive because they no longer spend time backing up their own files. Administrators and operators no longer need to support user-directed restores. These systematic backups ensure that data is safe, and recovery is quick if primary data is lost.

User-friendly and intuitive graphical user interfaces simplify both administration and use. An activity monitor and comprehensive logging and reporting reduce efforts in tracking and troubleshooting problems.

Master and media server domains along with the NetBackup media manager ensure that secondary storage devices are used to their best advantage. Backup storage is shared and managed automatically across the network. The broad range of device and media support also makes it easier to find suitable devices when adding storage capacity.

VERITAS NetBackup software was engineered for high performance, scalability, flexibility and ease of use. It is the ideal solution for backup, archiving and recovery of mission-critical data, which are the most critical storage management tasks for any organization.

APPENDIX A

FREQUENTLY ASKED QUESTIONS

1. Question: Does VERITAS NetBackup™ software provide full automation for backup and restore operations without operator intervention?

Answer: Yes. Operational involvement is not required if devices are configured and the needed media is online. Backups are performed by a scheduler process (not cron) based on administrator-specified schedules.

Users can restore files on demand through graphical or command line interfaces by perusing lists of backed up files and selecting which file(s) they want to restore. This selection is by file or directory name, and does not require any knowledge of the media involved. The server determines this automatically as part of the restoration process.

2. Question: Does VERITAS NetBackup software have the ability to restart a failed backup?

Answer: Yes. With frequency-based scheduling, automated backups begin in a specified period or backup window. VERITAS NetBackup software performs a specified number of retries, which is configurable, during the time the backup window is open.

3. Question: Does VERITAS NetBackup software provide media bar-code support?

Answer: Yes. VERITAS NetBackup software supports bar codes on robotic devices that contain bar-code readers.

4. Question: Which network protocols does VERITAS NetBackup software support?

Answer: VERITAS NetBackup software uses TCP/IP for transporting data.

5. Question: Does VERITAS NetBackup software allow users to exclude files from being backed up?

Answer: Yes. Each user may establish a unique “exclude list” of client files.

6. Question: Does VERITAS NetBackup software allow for backups to span tapes and tape devices?

Answer: Yes. With VERITAS NetBackup software, an individual tape or optical disk may contain multiple backups, and an individual backup may span multiple tapes or disks.

7. Question: Does VERITAS NetBackup software have the ability to create duplicate tape sets?

Answer: Yes. As a standard feature, VERITAS NetBackup software supports the creation of duplicate copies of the primary backup. A standard feature of the NetBackup software, Inline Copy enables the creation of up to four duplicate copies generated concurrently with the primary backup. A maximum of 10 duplicate copies can be created and maintained by VERITAS NetBackup™. The media used can be either disk or tape.

8. Question: What is the measured performance of both backup and restore operations for entire file systems with VERITAS NetBackup™ software?

Answer: There are many important variables that affect performance, such as network load, client and server capabilities, file system characteristics, file size and the number and type of peripherals configured.

9. Question: How many clients do your current customers typically back up on a single server? What is your experience in production with multiple NetBackup servers?

Answer: NetBackup media servers, operating under the control of a single master server, help decrease network traffic and make more peripherals available. Several current NetBackup customers are using

NetBackup servers to back up more than 5,000 clients. These customers are continually adding more client workstations to the configuration without experiencing any performance issues.

10. Question: What dynamic load balancing features does VERITAS NetBackup's scheduling process provide?

Answer: The NetBackup user can balance the network load by adjusting the "Limit jobs per policy" attribute of the client policy definition. This can give clients in one policy preference over those in another policy. If you group your client workstations by network location, this could balance networks of differing capabilities.

11. Question: Does VERITAS NetBackup software work simply and easily with a single tape drive if no robotic devices are available in the network?

Answer: Yes. VERITAS NetBackup, working in conjunction with VERITAS NetBackup EMM, provides an operator interface that tracks the status and mount requests for a standalone tape drive. Mounting previously labeled or used media will allow automatic assignment of a single drive.

The real advantage of VERITAS NetBackup EMM, however, is its powerful ability to coordinate multiple robotic peripherals, which lets you increase the capacity of small networks as your needs grow.

12. Question: Does VERITAS NetBackup software support the automatic scheduling of cleaning cartridges in robotic devices?

Answer: Yes. VERITAS NetBackup EMM supports automatic cleaning schedules in robotic tape devices and also tracks cleaning and usage information for devices that do not have mountable cleaning cartridges.

13. Question: Can VERITAS NetBackup software restore files to any machine regardless of original machine name or IP address in case the original machine no longer exists?

Answer: Yes. It is possible to restore files to alternate clients with VERITAS NetBackup software. An administrative action is necessary to allow this to happen, and the client user doing the restoration must identify the client from which the data was originally backed up.

14. Question: How is media handled if file backup and file migration are integrated?

Answer: The VERITAS NetBackup EMM is used as the common media management utility. This provides a common interface across all devices, whether cartridge tape or optical disk, and enables other programs and applications to share these devices.

15. Question: Does VERITAS NetBackup software support permanent logging of error messages?

Answer: Yes. VERITAS NetBackup software maintains a history of error messages in its error database. The default value is 28 days, but the administrator may modify this to provide a permanent record of the error message log.

16. Question: Can you generate catalog information about your backups from the backup media itself?

Answer: Yes. NetBackup software provides two different ways to perform this task. If the administrator follows the recommended procedures for backing up the NetBackup catalogs, the information contained is easily restored using the VERITAS NetBackup bprecover command. If these procedures are not followed, recovery takes longer but can be done by importing the media containing the database backups.

APPENDIX B

GLOSSARY

Administrator: A user granted special privileges to configure, install and manage VERITAS NetBackup software.

Archive: Duplicating a primary storage file in secondary storage, and then deleting the file from primary storage. Performed in order to retain data for a long period of time (also see “backup”).

Backup: Duplicating a primary storage file in secondary storage without deleting it from primary storage. Performed to protect data from system failures and accidental loss (also see “archive”).

Backup image: The collection of data VERITAS NetBackup™ software saves for a client during each backup or archive operation, including all associated files, directories and catalog information.

Backup window: The time during which automatic backups and user-directed backups and archives can occur.

Client policy: A group of clients designated by the administrator that shares common backup characteristics.

Command line interface: The client-based user interface provided by VERITAS NetBackup software to control backup and restore operations by means of individual commands and shell scripts (also see “graphical user interface,” “menu interface”).

Compression (software): The act of reducing the backup image size on the client to minimize data storage requirements and network traffic (also see “decompression”).

Daemon: A UNIX process, apart from the kernel, that performs a particular task.

Decompression: The act of reconstructing compressed data during a restore operation (also see “compression”).

Frequency: The designated time that should elapse between successful backups for a particular VERITAS NetBackup schedule.

Full backup: A backup of every specified file on a client (also see “incremental backup”).

Graphical User Interface (GUI): The administrator or client-based user interface provided by VERITAS NetBackup software conforming to OSF/Motif conventions (also see “menu interface,” “command line interface”).

Incremental backup: A backup of only specified client files that have been changed since the previous backup operation (also see “full backup”).

Master server: A server that performs all administrative actions and is responsible for all backup scheduling (also see “media server”).

Media server: A server operating under control of the master server that manages additional secondary storage units (also see “master server”).

Menu interface: The administrator or client-based user interface provided by VERITAS NetBackup software for individuals who do not have GUI capabilities (also see “graphical user interface,” “command line interface”).

Multiple volume device: A physical storage device not requiring manual intervention to change volumes because of built-in robotic controls (also see “single volume device”).

Multiplexing: Streaming data from multiple, simultaneous backups to the same device.

NetBackup domain: A single NetBackup master server and its associated media servers.

NFS mounts: Files residing on a remote node that are mounted on the local node through the Network File System (NFS) protocol.

Primary storage: Online magnetic disk storage connected directly to a client or server where new or active data is maintained (also see “secondary storage”).

Raw partition restore: Physical backup of a partition of a disk drive.

Removable media: A tape cartridge or optical disk that is not permanently mounted in a secondary storage device.

Restore: The act of returning a previously backed up or archived file to primary storage from secondary storage.

Retention level: A factor specifying how long backups or archives are to be saved before being deleted.

Robotic: Performing a complex mechanical task ordinarily assigned to NetBackup users, such as choosing one of several removable media and loading it into the drive of a secondary storage device.

Secondary storage: Supplemental storage connected to a storage server where data from primary storage is backed up or archived (also see “primary storage,” “removable media”).

Secure client: A client that does not require a /.rhosts file entry for the server (also see “trusting clients”).

Single volume device: Physical storage device requiring manual intervention to change volumes (also see “multiple volume device”).

Standalone device: Physical storage device requiring manual intervention to change volumes (also see “single volume device”).

Storage media: Any object on which data can be stored, such as tapes, tape cartridges and magnetic or optical disks.

Storage unit: As used by VERITAS NetBackup software, a logical entity that includes one or more storage devices that are of a specific type and media density and attach to a specific host.

True Image Restore (TIR): Restores only files that were in the directory at the date and time of a specific backup. Previously deleted files are ignored.

Trusting client: A client that has a /.rhosts file entry for the server (also see “secure clients”).

User: A person operating a client workstation (also see “administrator”).

Volume: Any physical storage medium such as a tape or optical disk.

VERITAS Software Corporation
Corporate Headquarters
350 Ellis Street
Mountain View, CA 94043
650-527-8000 or 866-837-4827

For additional information about VERITAS Software, its products, or the location of an office near you, please call our corporate headquarters or visit our Web site at www.veritas.com.